UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO INTERNACIONAL

“DERECHO INTERNACIONAL HUMANITARIO APLICADO A LA CIBERGUERRA: PRINCIPIOS REGULADORES”

TESIS PARA OBTENER EL TÍTULO DE LICENCIATURA EN DERECHO

PRESENTA

LEONARDO DAVID LIMA VALDÉS

ASESORA

DRA. ROSA JIMÉNEZ RODEA

CIUDAD UNIVERSITARIA, CIUDAD DE MÉXICO 2023

Agradecimientos

A mi hermana Aimeé, por su apoyo y cariño incondicional. Sin ti nada significaría lo mismo.

A mi madre y padre, por enseñarme a perseverar con fuerza.

A la Dra. Rosa Jiménez Rodea, por su confianza y apoyo constante para la elaboración de este trabajo.

A Max, Mon y Elizabeth, por su invaluable amistad, cariño y apoyo, así como por proveerme de discusiones constantes que nutrieron esta tesis. Gracias por acompañarme siempre.

A Mix y K, por su amistad y por el apoyo en momentos difíciles.

A Emilia, por su amor, compañía y apoyo.

A DHM, por todo.

Al equipo Jessup 123: Brayan, Ale, Diego, Ángel y Karen, en especial a Mariana y Velia, cuyo apoyo y confianza han sido muy importantes para mí.

Al equipo Jessup 369: Abril, Néstor y David, por su amistad, compañía y apoyo. He aprendido mucho con ustedes.

Al equipo Jessup 137: Emilia, Larissa y Diego, por su amistad y gran calidad humana, en especial a Arturo, por siempre ser tan bueno conmigo y aconsejarme.

A la comunidad Víctor Carlos García Moreno, por proveer el espacio académico que motivó esta tesis.

A la comunidad Philip C. Jessup, por enseñarme la pasión por el derecho internacional.

Índice

Introducción

El desarrollo tecnológico trae beneficios diversos en distintos ámbitos de la vida del ser humano. Sin embargo, es una moneda de dos caras: el anverso representa los beneficios y el reverso los peligros.

Los conflictos armados no son la excepción a los ámbitos que se ven transformados debido al progreso tecnológico. Tanto Estados como entes privados desarrollan capacidades cibernéticas con distintos propósitos. Las operaciones cibernéticas han sido empleadas dentro y fuera del contexto de un conflicto armado. Sus probados efectos llaman cada vez más la atención de la comunidad internacional.

Por ejemplo, en 2007, Israel bombardeó una instalación nuclear en Siria después de un ciberataque que neutralizó los radares terrestres y el sistema de defensa aérea. Por otro lado, durante el conflicto armado de 2008 entre Georgia y Rusia, los sitios *web* del gobierno y de los medios de comunicación de Georgia fueron desconectados o desfigurados durante las fases iniciales del conflicto, supuestamente por piratas informáticos rusos. Esto afectó la capacidad de comunicación de Georgia y posiblemente la operatividad de sus fuerzas armadas.[1]

Esta tesis tiene el propósito de dilucidar cómo es que el derecho internacional humanitario aplica al ciberespacio y qué instrumento pueden adoptar los Estados para sentar la base del desarrollo de la aplicación de este

[1] Cfr. ROSCINI, Marco, Cyber Operations and the Use of Force in International Law, S.N.E., Oxford University Press, Reino Unido, 2014, pág. 7123.

régimen a la ciberguerra. Esto con la finalidad de presentar una guía clara para que los Estados acaten las normas aplicables durante la conducción de las hostilidades.

Actualmente, la regulación del uso de capacidades cibernéticas en la conducción de las hostilidades se encuentra en una zona gris. Algunos actores asumen que el derecho internacional humanitario aplica al ciberespacio y que solamente falta que sea respetado. Otros sostienen que se requiere la creación de un instrumento particular. El punto medio es que el derecho internacional humanitario sí aplica al ciberespacio y sólo hace falta una visión clara sobre cómo se aplica, debido a las peculiaridades de este ámbito.

Sobre el particular, el presente trabajo se abocará a demostrar que el derecho internacional humanitario aplica a la guerra cibernética y que la mejor forma de desarrollar su aplicación es mediante la práctica estatal guiada a través de un instrumento jurídico consensuado por la comunidad internacional.

Bajo ese entendido, esta tesis se divide en cuatro capítulos: 1) marco teórico del derecho internacional humanitario, 2) ciberguerra, 3) el derecho internacional humanitario y la ciberguerra, y 4) un nuevo instrumento jurídico para afirmar la aplicación de los principios reguladores del derecho internacional humanitario en la ciberguerra.

En el primer capítulo, se describe de forma breve el funcionamiento y el alcance del derecho internacional humanitario actual. Este capítulo sienta la base teórica necesaria para estudiar la aplicación del derecho internacional humanitario al ciberespacio. Además, muestra que, si bien la comunidad

internacional pone cada vez más atención a la ciberguerra, lo cierto es que no hay una perspectiva clara sobre su aplicación.

En el segundo capítulo, se explican los aspectos técnicos de las operaciones cibernéticas en general, ya sea en tiempo de paz o de guerra. Asimismo, se aborda la recepción de las operaciones cibernéticas en el derecho internacional humanitario, es decir, qué elementos de estas operaciones pueden ser regulados como medios o como métodos para hacer la guerra.

En el tercer capítulo, se expone cómo es que el derecho internacional humanitario aplica a la regulación del uso de medios y métodos de guerra cibernética, tanto en el desarrollo técnico de éstos como en el momento de desplegarlos en combate. Esta explicación se centra en el artículo 36 del "Protocolo Adicional I a los Convenios de Ginebra" y en los principios reguladores del derecho internacional humanitario: distinción, proporcionalidad, necesidad militar y humanidad.

En el cuarto capítulo, se abordan algunas posturas y propuestas respecto de la necesidad de adoptar un nuevo instrumento jurídico que regule la conducción de la ciberguerra. Esto con el objetivo de llegar a una propuesta final sobre la manera más adecuada, según el desarrollo de esta tesis, de regular el derecho internacional humanitario aplicado al ciberespacio.

Capítulo 1. Marco teórico del derecho internacional humanitario

El propósito de este capítulo es exponer el alcance que actualmente tiene el derecho internacional humanitario convencional y consuetudinario sobre la regulación de la conducción de las hostilidades en los distintos tipos de conflictos armados y en relación con los medios y métodos de guerra que pueden ser empleados.

1.1 Derecho internacional humanitario y ciberguerra

Es preciso entender a qué nos referimos con derecho internacional humanitario, también conocido como el derecho de los conflictos armados o de la guerra. El derecho internacional humanitario también es identificado como *jus in bello*, pues es el derecho aplicable en los conflictos armados. El derecho internacional humanitario se distingue del derecho del uso de la fuerza, conocido como *jus ad bellum*, referente al derecho a recurrir a un conflicto armado.[2] Por lo tanto, el derecho internacional humanitario regula únicamente la conducción de los conflictos armados, no el cómo y cuándo se inició el conflicto.[3]

En conexión con lo anterior, este capítulo resalta aquellas reglas del derecho internacional humanitario aplicables a la ciberguerra. En esta investigación se entenderá, preliminarmente, que ciberguerra significa: “defender

[2] Cfr. SAUL, Ben y AKANDE, Dapo (eds.), The Oxford Guide to International Humanitarian Law, S.N.E., Oxford University Press, New York, 2020, pág. 1.
[3] Cfr. CRWE, Jonathan y WESTON-SCHEUBER, Kylie, Principles of International Humanitarian Law, S.N.E., Edward Elgar Publishing Limited, Cheltenham, 2013, pág. 7.

y atacar información y redes informáticas, así como negar la capacidad del adversario para hacer lo mismo, o incluso dominar el entorno de la información en el campo de batalla".[4]

En ese tenor, la ciberguerra se desarrolla en el ciberespacio, que es "un dominio global dentro del entorno de la información que consiste en las redes interdependientes de las infraestructuras de la tecnología de la información y los datos residentes, lo que contempla el *internet*, las redes de telecomunicaciones, los sistemas informáticos, los procesadores y los controladores integrados".[5] Esta acepción se utilizará de forma inicial y sujeta al desarrollo posterior en el capítulo segundo.

Es así como, para comprender cómo funciona el derecho internacional humanitario y, en consecuencia, cómo se puede aplicar a la ciberguerra, es debido abordar las fuentes del derecho internacional humanitario, su contexto de aplicación y su objeto de regulación.

1.2. Fuentes del derecho internacional humanitario

1.2.1. Derecho internacional humanitario convencional

[4] Cfr. HILDRETH, Steven A., CRS Report for Congress Cyberwarfare, The Library of Congress, 2001, pág. 1, nota al pie 3: "…defending and attacking information and computer networks, as well as denying an adversary's ability to do the same, or even dominating the information environment on the battlefield".

[5] Cfr. OFFICE OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF, DOD Dictionary of Military and Associated Terms, Washington DC, 2021, pág. 55: "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

El desarrollo convencional del derecho internacional humanitario puede dividirse en tres rubros, según el lugar de su desarrollo: La Haya, Ginebra y Nueva York.

a) La Haya

Sobre el desarrollo del derecho internacional humanitario en La Haya, hay dos conferencias principales: la primera del 18 de mayo al 29 de julio de 1899; la segunda del 15 de junio al 18 de octubre de 1907.[6] Resultado de las conferencias se concluyó la "Convención relativa a las leyes y costumbres de la guerra terrestre", así como el "Reglamento relativo a las leyes y costumbres de la guerra terrestre", ambas de 1907.

Los aspectos más relevantes del reglamento referido son: los elementos para determinar qué milicias y cuerpos de voluntarios son combatientes —artículo 1—;la protección especial para los combatientes que fueran capturados como prisioneros de guerra —artículo 3—;la limitación en la elección de medios para dañar a la parte enemiga —artículo 22—,así como la prohibición de emplear ciertas armas —artículo 23—y en particular aquellas que causan males innecesarios —artículo 23(e)—; y, las primeras reglas sobre la protección de objetos por su importancia cultural o médica —artículo 27—.

Además, la "Convención de la Haya" de 1907 incorporó en su preámbulo la hoy conocida "Cláusula Martens", que establece una forma de protección residual: "Mientras que se forma un Código más completo de las leyes de la

[6] Cfr. LIVOJA, Rain y McCORMACK, Tim (eds.), Routledge Handbook of the Law of Armed Conflict, S.N.E., Routledge, New York, 2016, pág. 37.

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".

Igualmente, se adoptaron Convenciones en torno a la guerra marítima, *v.gr.*: "Convención para la adaptación de los principios de la Convención de Ginebra a la guerra marítima"; "Convención relativa a ciertas restricciones en cuanto al ejercicio de derecho de captura en la guerra marítima"; "Convención relativa a la colocación de minas submarinas automáticas de contacto"; y, "Convención IX de La Haya relativa al bombardeo por las fuerzas navales en tiempo de guerra".

En 1923, en la Haya, la Comisión de Juristas Internacional, establecida en 1922 por Estados Unidos de América, Gran Bretaña, Francia, Italia y Japón, generó las "Reglas de la guerra aérea". A pesar de que esta normativa no llegó a ser vinculante, algunas de sus reglas fueron retomadas por los Estados en la práctica.[7] En particular, las "Reglas de la guerra aérea" de 1923 establece que únicamente objetivos militares podían ser atacados —artículo 22—.Esta provisión fue reafirmada posteriormente por la Asamblea de la Liga de las Naciones Unidas.[8]

[7] Cfr. LIVOJA, Rain y McCORMACK, Tim (eds.), Routledge Handbook of the Law of Armed Conflict, *Op. Cit.*, pág. 41.
[8] *Ibidem,* pág. 42.

Luego, en 1954, una conferencia intergubernamental convocada por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, adoptó la “Convención para la protección de los bienes culturales en caso de conflicto armado”. Esta Convención es aplicable tanto en conflictos armados internacionales como no internacionales —artículo 19—.

Adicionalmente, se adoptó el “Protocolo para la protección de los bienes culturales en caso de conflicto armado” y el “Segundo Protocolo de la Convención de La Haya de 1954 para la Protección de los Bienes Culturales en caso de Conflicto Armado”.

b) Ginebra

En 1864, en Ginebra, se adoptó el primer convenio denominado “Convenio de Ginebra del 22 de agosto de 1864 para el mejoramiento de la suerte de los militares heridos en los ejércitos en campaña”.

Esta convención se enfocó en los siguientes aspectos:[9] los combatientes heridos y enfermos serían recogidos y cuidados sin importar su nacionalidad; las ambulancias y hospitales militares que cuidaran de los combatientes serían reconocidos como neutrales, por ende, respetados y protegidos; la población local que recogiera heridos estaría igualmente protegida, permanecería libre; y, adoptarían el signo distintivo de la Cruz Roja.

[9] *Ibidem*, pág. 34.

El “Convenio II de Ginebra para mejorar la suerte de los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar”,[10] adoptado en 1906, se centró en la condición de herido y enfermo del personal militar y las sociedades de ayuda voluntaria, además del rol del personal sanitario.

De igual manera, el “Protocolo sobre la prohibición del uso en la guerra, de gases asfixiantes, tóxicos o similares y de medios bacteriológicos” fue adoptado en 1925 en Ginebra, y en 1972 fue complementado por la “Convención sobre la prohibición del desarrollo, la producción y el almacenamiento de armas bacteriológicas (biológicas) y toxínicas y sobre su destrucción”, negociada en Ginebra por el Comité sobre Desarme.

Por otra parte, en 1929, tuvo lugar una conferencia diplomática en Ginebra que resultó en la adopción de dos Convenios: el “Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña” y el “Convenio de Ginebra relativo al trato debido a los prisioneros de guerra”.

El primero, reemplazó al “Convenio sobre los heridos y enfermos” de 1906 y estableció que el Convenio debía ser respetado en todas las circunstancias —artículos 1 y 59—. El segundo, completó las disposiciones análogas en las “Regulaciones de la Haya” de 1907; particularmente, prohibió cualquier tipo de reprimendas en contra de los prisioneros de guerra —artículo 2—.

Posteriormente, en 1949, se adoptaron 4 Convenios resultado de una conferencia diplomática en Ginebra. Tres de ellos reemplazaron a los de 1906 y

[10] *Ibidem*, págs. 39-40.

1929, mientras que el cuarto convenio fue el primero en abordar específicamente la protección de las personas civiles. En ese sentido, los cuatro Convenios son relativos a los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar; a los prisioneros de guerra y a las personas civiles protegidas en tiempo de guerra.[11]

Los cuatro convenios contienen 3 artículos comunes: el primero, referente al respeto de estos instrumentos en todas las circunstancias; el segundo, respecto de su aplicación en cualquier conflicto; y el tercero, prevé las reglas mínimas de trato a las partes en un conflicto armado no internacional en el territorio de un Estado.

Adicionalmente, en 1977, se adoptaron los siguientes instrumentos internacionales: el "Protocolo I adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales", en adelante "Protocolo Adicional I a los Convenios de Ginebra", y 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", en adelante "Protocolo Adicional II a los Convenios de Ginebra".

El "Protocolo Adicional I a los Convenios de Ginebra" contiene regulaciones respecto de: heridos, enfermos y náufragos; medios y métodos de guerra; estatuto de combatiente y de prisionero de guerra; y, protección a la población y bienes civiles.

[11] Cfr. KALSHOVEN, Frits y ZEGVELD, Liesbeth, Restricciones en la conducción de la guerra: introducción al derecho internacional humanitario, 2ª ed., Comité Internacional de la Cruz Roja, trad. Margarita Polo, Buenos Aires, 2005, págs. 31-32.

El “Protocolo Adicional II a los Convenios de Ginebra”, de forma paralela al “Protocolo Adicional I a los Convenios de Ginebra”, regula la protección a los heridos, enfermos y náufragos, así como a la población y bienes civiles. Asimismo, dispone la obligatoriedad del trato humano debido a todas las personas en el contexto del conflicto armado. Sin embargo, no contiene apartados específicos sobre medios y métodos de guerra, o sobre combatientes y prisioneros de guerra.

Asimismo, se adoptó el “Protocolo III adicional a los Convenios de Ginebra de 1949 relativo a la aprobación de un signo distintivo adicional”, donde se aprobó el uso del cristal rojo como emblema extra al de la cruz roja y media luna roja, como un signo distintivo neutral sin posible connotación religiosa o política.

En 1980, se adoptó la “Convención sobre prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados”. Actualmente, esta convención aplica tanto en conflictos armados internacionales como no internacionales, toda vez que, en 2001, los Estados parte decidieron ampliar su alcance.

Asimismo, esta Convención tiene 5 protocolos adicionales que regulan: fragmentos no localizables (Protocolo I); el empleo de minas, armas trampa y otros artefactos (Protocolo II); el empleo de armas incendiarias (Protocolo III); armas láser cegadoras (Protocolo IV); y, los restos explosivos de guerra (Protocolo V). El campo de aplicación de estos protocolos también se extendió en 2001 a los dos tipos de conflictos armados.

Adicionalmente, en 1992, en Ginebra, la Conferencia sobre Desarme adoptó la “Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas y sobre su Destrucción”.

c) Nueva York

En relación con el derecho internacional humanitario desarrollado en Nueva York, se hace referencia particularmente al trabajo de Naciones Unidas en torno al derecho internacional humanitario.

En principio, Naciones Unidas se mostró renuente sobre la inclusión del derecho internacional humanitario en sus programas de trabajo. Sin embargo, contribuyó en cierta medida a su desarrollo mediante el establecimiento de tribunales para enjuiciar a criminales de guerra:[12] como el Tribunal de Núremberg en 1945 y el Tribunal de Tokio en 1946.

En la “Resolución 1 (I)”, Naciones Unidas estableció una Comisión para lidiar con los problemas creados por el descubrimiento de la energía nuclear, con el objetivo de hacer propuestas para eliminar las armas nucleares de los armamentos estatales, así como cualquier otra arma de destrucción masiva.[13]

[12] *Ibidem*, pág. 33.

[13] Cfr. PRIMERA COMISIÓN DE NACIONES UNIDAS SOBRE DESARME Y SEGURIDAD INTERNACIONAL, “Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy”, Resolución 1(I), Décimo primera sesión plenaria, 24 de enero de 1946, párr. 5 c).

Por otro lado, en la “Resolución 1653 (XVI)”[14] Naciones Unidas se pronunció en pro de la prohibición del uso de armas nucleares.

En 1968, Naciones Unidas adoptó una postura más activa sobre el derecho aplicable en conflictos armados. Como resultado de la Conferencia Internacional de Derechos Humanos, reunida del 22 de abril al 15 de mayo de 1968 en Teherán, se aprobó la “Resolución XXIII” sobre los derechos humanos en los conflictos armados.

Esta resolución, adoptada bajo los auspicios de Naciones Unidas, instó al Secretario General de esta organización a estudiar la aplicación del derecho internacional humanitario del momento y la posibilidad de ampliar el derecho convencional existente, con la finalidad de asegurar una mejor protección de las personas civiles, personas prisioneras de guerra y combatientes en todos los conflictos armados, así como la prohibición y la restricción del empleo de ciertos medios y métodos de hacer la guerra.[15]

En consonancia, la Asamblea General de Naciones Unidas respaldó dicha propuesta mediante la “Resolución 2444 (XXIII)” sobre el respeto por los derechos humanos en conflictos armados,[16] a la vez que sentó los tres principios básicos sobre los cuáles, según la Asamblea General de Naciones Unidas, se

[14] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Declaration on the prohibition of the use of nuclear and thermo-nuclear weapons”, Resolución 1653 (XVI), Décimo sexto período de sesiones, 24 de noviembre de 1961, párr. 1 b).
[15] Cfr. KALSHOVEN, Frits y ZEGVELD, Liesbeth, Restricciones en la conducción de la guerra: introducción al derecho internacional humanitario, *Op. Cit.*, págs. 34-35.
[16] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Respect for human rights in armed conflicts”, Resolución 2444 (XXIII), Vigésimo tercer período de sesiones, 19 de diciembre de 1968.

debía guiar la futura codificación del derecho internacional humanitario, a saber:[17] el derecho limitado de las partes beligerantes a elegir medios y métodos de guerra, la prohibición de ataques sobre la población civil y el principio de distinción entre combatientes y no combatientes.

Posteriormente, el Secretario General y la Asamblea General de Naciones Unidas incluyeron el estudio del derecho internacional humanitario en sus áreas de interés. El primero, mediante la elaboración de informes anuales; mientras que, el segundo, a través de la aprobación de resoluciones sobre temas específicos como la protección de mujeres y niños, así como la condición de combatientes en guerras de liberación nacional.[18]

De esta forma, bajo auspicios de Naciones Unidas, se adoptó en 1997, la "Convención sobre la prohibición del empleo, almacenamiento, producción y transferencia de minas antipersonal y sobre su destrucción." Por separado, en la Conferencia Diplomática de Dublín, se adoptó la "Convención de 2008 sobre Municiones de Racimo", donde el Secretario General de Naciones Unidas es el depositario.

Asimismo, Naciones Unidas se involucró en el desarrollo del derecho internacional humanitario enfocado en la protección del medio ambiente. Ejemplo de esto es la adopción de la "Convención sobre la prohibición de utilizar técnicas

---

[17] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, "*The United Nations and International Humanitarian Law: The International Committee of the Red Cross and the United Nations' involvement in the implementation of international humanitarian law*", en International Committee of the Red Cross, Ginebra, Suiza, 19 de octubre de 1995, [en línea] https://www.icrc.org/en/doc/resources/documents/misc/57jmuk.htm.

[18] Cfr. KALSHOVEN, Frits y ZEGVELD, Liesbeth, Restricciones en la conducción de la guerra: introducción al derecho internacional humanitario, *Op. Cit.*, pág. 35

de modificación ambiental con fines militares u otros fines hostiles" por la Asamblea General de Naciones Unidas en 1976, por medio de la "Resolución 31/72".[19]

Igualmente, en 2011, la Embajadora Marie G. Jacobsson propuso a la Comisión de Derecho Internacional de Naciones Unidas la inclusión del tema "Protección del medio ambiente en relación con conflictos armados".[20] En 2013, la Comisión de Derecho Internacional lo incluyó en su programa de trabajo y la Embajadora Marie Jacobsson fue elegida Relatora Especial.[21] Actualmente, este tópico aún se encuentra bajo consideración, pero está próximo a alcanzar su conclusión.[22]

Por otro lado, la Asamblea General de Naciones Unidas decidió crear un Grupo de Trabajo de Composición Abierta en 2018, que aborda el tema de "Avances en la Esfera de la Información de las Telecomunicaciones en el Contexto de la Seguridad Internacional".[23] En 2021, este grupo concluyó que dentro de las amenazas existentes y potenciales a la paz y seguridad internacional se encuentra el hecho de que los Estados desarrollan cada vez más

---

[19] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Establishment of a nuclear-weapon-free zone in the region of the Middle East", Resolución 31/71, Trigésimo primer período de sesiones, 10 de diciembre de 1976.

[20] Cfr. COMISIÓN DE DERECHO INTERNACIONAL, "Report of the International Law Commission to the Sixty-Third Session, Annex E. Protection of the Environment in Relation to Armed Conflicts", Documento de Naciones Unidas A/66/10, 26 de abril-3 de junio y 4 de julio-12 de agosto de 2011, pág. 215, párr. 31.

[21] Cfr. JACOBSSON, Marie y MARJA, Lehto, "*Protection of the Environment in Relation to Armed Conflicts – An Overview of the International Law Commission's Ongoing Work*", en Goettingen Journal of International Law, Alemania, 2020, Vol. 10, Núm. 1,17 de julio del 2020, pág. 29.

[22] *Ibidem*, pág. 45.

[23] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Developments in the field of information and telecommunications in the context of international security", Resolución 73/27, Septuagésimo tercer período de sesiones, 5 de diciembre de 2018, pág. 5, párr. 5.

sus capacidades en el campo de las tecnologías de la información y la comunicación con propósitos militares.[24]

Igualmente, Naciones Unidas estableció un Grupo de Expertos Gubernamentales sobre el desarrollo en el campo de las tecnologías de la información y la comunicación en el contexto de la seguridad internacional. Este grupo concluyó en 2015, que los principios de humanidad, necesidad, proporcionalidad y distinción aplican al uso que los Estados dan a las tecnologías de la información y la comunicación.[25]

Subsecuentemente, la Asamblea General de Naciones Unidas requirió a su Secretario General que estableciera un Grupo de Expertos Gubernamentales con el objetivo de desarrollar el tópico avances en la información y las telecomunicaciones en el contexto de la seguridad internacional".[26]

En consideración de cómo aplica el derecho internacional al uso de las tecnologías de la información y telecomunicaciones, en 2021, el grupo resaltó que el derecho internacional humanitario únicamente aplica en situaciones de conflicto armado. Asimismo, confirmó la aplicación de los principios de humanidad, necesidad, proporcionalidad y distinción. Sin embargo, reconoció

[24] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Open-ended working group on developments in the field of information and telecommunications in the context of international security", Documento de Naciones Unidas A/AC.290/2021/CRP.2, Documento de la sala de conferencias del 10 de marzo de 2021, párrs. 16-17.

[25] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", Documento de Naciones Unidas A/70/174, Septuagésimo período de sesiones, 22 de julio de 2015, pág. 13, párr. 28 d).

[26] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Advancing responsible State behaviour in cyberspace in the context of international security", Resolución 73/266, Septuagésimo tercer período de sesiones, 22 de diciembre de 2018, párr. 3.

que el tema de cómo y cuándo aplican estos principios aún requiere mayor estudio.[27]

1.2.2. Derecho internacional humanitario consuetudinario

En 1995, la Conferencia Internacional de la Cruz Roja y de la Medialuna Roja encomendó al Comité Internacional de la Cruz Roja la preparación de un reporte sobre las normas consuetudinarias de derecho internacional humanitario que fueran aplicables tanto en conflictos armados internacionales como no internacionales.[28] Como resultado, en 2005, se publicaron las reglas[29] y prácticas[30] relativas al derecho internacional humanitario consuetudinario.

El estudio del Comité Internacional de la Cruz Roja formuló 161 reglas consuetudinarias del derecho internacional humanitario; donde 149 son aplicables a conflictos armados no internacionales y 159 son aplicables a conflictos armados internacionales.[31] Es decir, la mayoría de las reglas consuetudinarias empalman su aplicación en ambos tipos de conflictos.

---

[27] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", Documento de Naciones Unidas A/76/135, Septuagésimo sexto período de sesiones, 14 de julio de 2021, pág. 18, párr. 71 f).

[28] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, 26th International Conference of the Red Cross and Red Crescent – Resolutions (and annexes), International Review of the Red Cross, ICRC, Ginebra, 1995, No. 310, Enero-Febrero 1996, pág. 84.

[29] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, S.N.E., Cambridge University Press, Cambridge, 2005.

[30] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume II: Practice – Part 1 and Part 2, S.N.E., Cambridge University Press, Cambridge, 2005.

[31] Cfr. LIVOJA, Rain y McCORMACK, Tim (eds.), Routledge Handbook of the Law of Armed Conflict, *Op. Cit.*, pág. 79.

La relevancia del derecho internacional humanitario consuetudinario se deriva de su aplicación vinculante y generalizada en los conflictos armados. En ese sentido, en ocasiones se ha referido que los principios fundamentales del derecho internacional humanitario tienen una base triple en las fuentes del derecho internacional: emanan de tratados y costumbre internacional, a la vez que constituyen principios generales de derecho.[32] Esta sección se centrará en los principios del derecho internacional humanitario como costumbre.

Lo anterior, debido a que estos principios expresan la sustancia del derecho internacional humanitario y sirven de directrices en los casos no previstos.[33] Consecuentemente, son de observancia obligatoria incluso para los Estados no parte de los convenios relativas al derecho internacional humanitario.[34]

Como la Corte Internacional de Justicia consideró en el caso "*Actividades militares y paramilitares en y contra Nicaragua*", los principios generales fundamentales del derecho internacional humanitario pueden ser vistos como la base del desarrollo convencional del derecho internacional humanitario; o bien, este derecho convencional puede ser visto únicamente como expresión de estos principios.[35]

---

[32] *Ibidem*, pág. 82.

[33] Cfr. PICTET, Jean, "Développement et príncipes du droit international humanitaire", citado por SALMÓN, Elizabeth, Introducción al Derecho Internacional Humanitario, 3ª ed., Comité Internacional de la Cruz Roja, Perú, Lima, 2012, pág. 56.

[34] Cfr. CORTE INTERNACIONAL DE JUSTICIA, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Estados Unidos de América). Sentencia de juicio de 27 de junio de 1986. I.C.J. Reports 1986, págs. 113-114, párr. 218.

[35] *Ibidem*, párr. 220.

Al respecto, en la conducción de las hostilidades, las partes beligerantes deben distinguir entre objetivos militares y civiles, es decir, tienen que actuar con precaución. Al mismo tiempo, el derecho internacional humanitario exige un análisis constante de la proporcionalidad entre necesidad militar y humanidad. Este balance continuo sirve para determinar si un ataque ilícito, en principio, puede ser legítimo según las circunstancias o si un ataque causaría daños innecesarios.

La Corte Internacional de Justicia identificó el "Principio de distinción" y la "Prohibición de causar sufrimiento innecesario" como principios cardinales del derecho internacional humanitario.[36] Por lo tanto, su aplicación es constante en cada operación militar.

Sobre el "Principio de Distinción", las partes de un conflicto siempre deben diferenciar entre civiles y combatientes. Los ataques únicamente pueden dirigirse contra combatientes, nunca contra civiles.[37] Igualmente, siempre se debe distinguir entre objetos civiles y objetivos militares. Sólo es permisible realizar ataques contra objetivos militares.[38] En ese tenor, el ataque a un objetivo civil únicamente sería permisible bajo un supuesto donde la necesidad militar sea más grande que la afectación al "Principio de Humanidad".

El principio más importante del derecho internacional humanitario es el de distinción debido a que establece el límite que no deben traspasar las partes

[36] Cfr. CORTE INTERNACIONAL DE JUSTICIA, Legality of The Threat or Use of Nuclear Weapons. Opinión Consultiva de 8 de julio de 1996. I.C.J. Reports 1996, pág. 257, párr. 78.
[37] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 1, pág. 3.
[38] Cfr. *Ibidem*, Regla 7, pág. 25.

beligerantes. Anejo a este principio se encuentra el "Principio de Precaución", que implica que las partes de un conflicto armado deben evitar o, en su caso, minimizar el daño incidental sobre personas y objetos protegidos.[39]

Así, de haber daño incidental, debe ser proporcional, lo que comprende que la afectación a bienes y personas civiles debe ser menor a la ventaja militar anticipada concreta y directa que se busca obtener; mientras que, la necesidad militar justifica las medidas de violencia militar que son necesarias y proporcionadas para garantizar el rápido sometimiento del enemigo con el menor costo posible en vidas humanas y recursos económicos.[40]

Es debido marcar la distinción entre necesidad militar y ventaja militar. La primera se refiere a si el ataque es indispensable o no, mientras que la segunda comprende lo indispensable del ataque y la ganancia, superioridad u oportunidad obtenida.[41] El "Principio de Necesidad Militar" opera exclusivamente como una excepción, al autorizar un comportamiento que se desvía de las conductas apegadas al derecho internacional humanitario.

---

[39] Cfr. MELZER, Nils, International Humanitarian Law: A Comprehensive Introduction, S.N.E., International Committee of the Red Cross, Suiza, Ginebra, 2019, pág. 18; Cfr. KOLB, Robert, Advanced Introduction to International Humanitarian Law, S.N.E., Edward Elgar Publishing Limited, Reino Unido, Cheltenham, 2014, pág. 81.

[40] Cfr. SALMÓN, Elizabeth, Introducción al Derecho Internacional Humanitario, 3ª ed., Comité Internacional de la Cruz Roja, Perú, Lima, 2012, pág. 60; Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 14, pág. 46; Cfr. MELZER, Nils, International Humanitarian Law: A Comprehensive Introduction, *Op. Cit.*, pág. 19.

[41] Cfr. LIVOJA, Rain y McCORMACK, Tim (eds.), Routledge Handbook of the Law of Armed Conflict, *Op. Cit.*, pág. 91.

Por otro lado, al describir el “Principio de Humanidad”, se le ha relacionado con el contenido de la “Cláusula Martens”.[42] A tal efecto, la esta cláusula va en contra de la concepción de que todo lo que no está prohibido, está permitido.[43] Es decir, cuando no haya regla específica aplicable, se estará a lo dispuesto por los usos establecidos entre las naciones civilizadas, por las leyes de la humanidad y por las exigencias de la conciencia pública, que en otras palabras implica tratar con humanidad.

Respecto de la prohibición de causar sufrimiento innecesario, las partes beligerantes tienen prohibido utilizar armas que causen daño innecesario o que agraven el sufrimiento inútilmente.[44] En consecuencia, para saber si el daño es innecesario, la proporcionalidad entre la humanidad del ataque y la necesidad militar son cruciales.

La prohibición de causar daño innecesario o superfluo a los combatientes comprende la prohibición o restricción sobre el uso de medios o métodos de guerra que puedan causar ese tipo de efectos.[45] El “Principio de Humanidad” da vida al “Principio de prohibición de causar daños superfluos o sufrimientos innecesarios”.[46] Sobre el particular, el respeto por estos principios dio lugar a las convenciones que prohíben armas específicas.

---

[42] Cfr. KOLB, Robert, Advanced Introduction to International Humanitarian Law, *Op. Cit.*, pág. 78; Cfr. LIVOJA, Rain y McCORMACK, Tim (eds.), Routledge Handbook of the Law of Armed Conflict, *Op. Cit.*, pág. 93.
[43] Cfr. KOLB, Robert, Advanced Introduction to International Humanitarian Law, *Op. Cit.*, pág. 79.
[44] Cfr. CORTE INTERNACIONAL DE JUSTICIA, Legality of The Threat or Use of Nuclear Weapons, *Op. Cit.*, pág. 257, párr. 78.
[45] Cfr. MELZER, Nils, International Humanitarian Law: A Comprehensive Introduction, *Op. Cit.*, pág. 19.
[46] Cfr. SALMÓN, Elizabeth, Introducción al Derecho Internacional Humanitario, *Op. Cit.*, pág. 61.

1.3. Contexto de aplicación

La aplicación del derecho internacional humanitario varía en torno al tipo de conflicto armado que se presenta: conflicto armado internacional o conflicto armado no internacional. En ese sentido, se abordarán los dos tipos de conflictos que se pueden generar y los elementos característicos de cada uno.

La creación de los cuatro "Convenios de Ginebra de 1949" dio inicio a la diferenciación entre conflictos armados internacionales y no internacionales, derivado de sus artículos 2 y 3 comunes a los cuatro convenios.

Posteriormente, dicha división se asentó con la adopción de los protocolos adicionales de 1977 a los "Convenios de Ginebra de 1949".[47] El primero se dedicó a la protección de las víctimas de los conflictos armados internacionales y el segundo a las víctimas de los conflictos armados no internacionales.

1.3.1. Conflicto armado internacional

Aunque no existe una definición convencional sobre qué constituye un conflicto armado internacional, el artículo 2 común a los cuatro "Convenios de Ginebra de 1949" refiere que su aplicación se limita a un caso de "(…) guerra declarada o de cualquier otro conflicto armado que surja entre dos o varias de las Altas Partes Contratantes, aunque una de ellas no haya reconocido el estado de guerra".

[47] Cfr. SAUL, Ben y AKANDE, Dapo (eds.), The Oxford Guide to International Humanitarian Law, *Op. Cit.*, pág. 30.

Asimismo, un conflicto armado existe porque la guerra ha sido declarada o porque las condiciones fácticas permiten identificar la existencia de un conflicto armado.[48]

Sobre el particular, el comentario a dicho artículo menciona que un conflicto armado internacional[49] es "cualquier diferencia que surja entre dos Estados y que dé lugar a la intervención de miembros de las fuerzas armadas (…)".[50]

En el caso "*Tadic*", el Tribunal Penal Internacional para la Antigua Yugoslavia determinó que "(…) existe un conflicto armado cuando se recurre a la fuerza armada entre Estados (…)".[51] Esta definición de un conflicto armado internacional ha sido retomada en diversas ocasiones por tribunales internacionales.

Así, no se requiere que el conflicto se extienda en el tiempo o que haya un número determinado de víctimas. Únicamente se necesita que el uso de la fuerza armada esté motivado por la intención de causar daño a la parte enemiga.[52] Por

---

[48] *Ibidem*, pág. 33.

[49] Cfr. BARTELS, Rogier, "*Timelines, borderlines and conflicts: The historical evolution of the legal divide between international and non-international armed conflicts*", en International Review of the Red Cross, ICRC, Geneva, 2009, Vol. 91, No. 873, marzo 2009, pág. 38.

[50] PICTET, Jean S., Commentary on the Geneva Conventions of 12 August 1949 relative to the Treatment of Prisoners of War, S.N.E., ICRC, trad. A. P. de Heney, Geneva, 1960, pág. 23: "Any difference between two States and leading to the intervention of members of the armed forces…".

[51] TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Dusko Tadic. Decisión sobre la moción de la defensa para la apelación interlocutoria sobre jurisdicción de 2 de octubre de 1995. Caso No. IT-94-1-A, párr. 70: "…an armed conflict exists whenever there is a resort to armed force between States…".

[52] Cfr. VITÉ, Silvain, "*Typology of armed conflicts in international humanitarian law: legal concepts and actual situations, International Review of the Red Cross*", en International Review of the Red Cross, Geneva, Vol. 91, Núm. 873, marzo 2009, pág. 72.

lo tanto, resultan irrelevantes las razones o la intensidad del enfrentamiento,[53] pues el sólo uso de la fuerza entre Estados configura el conflicto armado.

Por otro lado, la aplicación del "Protocolo Adicional I a los Convenios de Ginebra" extiende la caracterización de un conflicto armado internacional cuando "(…) 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 (…)".[54]

1.3.2 Conflicto armado no internacional

Un conflicto armado no internacional existe cuando hay "(…) violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre estos grupos dentro de un Estado".[55]

Al respecto, esta definición se compone de dos elementos:[56] a) violencia armada prolongada o intensidad del conflicto, y b) que las partes involucradas en el conflicto estén organizadas.

---

[53] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, How is the Term "Armed Conflict" Defined in International Humanitarian Law?, Opinion Paper, Geneva, marzo 2008, pág. 1.

[54] "Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I)", *Op. Cit.*, art. 1(4).

[55] TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Dusko Tadic, *Op. Cit.*, párr. 70: "…protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".

[56] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Ramush Haradinaj, Idriz Balaj, and Lahi Brahimaj. Sentencia de fondo de 3 de abril de 2008. Caso No. IT-04-84-T, párr. 38.

La identificación de estos dos elementos cobra relevancia al momento de excluir disturbios civiles o actos aislados de terrorismo,[57] así como otros actos de bandidaje o insurrecciones desorganizadas y efímeras, ya que estas otras actividades no están sujetas al derecho internacional humanitario.[58]

En torno a la intensidad del conflicto, los elementos que sirven para su valoración son los siguientes:[59] tanto la seriedad como la cantidad de ataques, su alcance territorial y temporal, el incremento de fuerzas gubernamentales, la distribución de armas entre las partes del conflicto, así como la atención que haya atraído del Consejo de Seguridad de Naciones Unidas y, si es que hay, resoluciones de este órgano en relación con el conflicto armado.

Asimismo, es relevante considerar la manera en que los órganos estatales hacen uso de la fuerza en contra de los grupos armados, pues las normas vinculantes sobre su conducta varían en función de si se identifica una situación de conflicto armado o no.[60]

Por otro lado, con respecto a la organización de las partes involucradas, algunos elementos para valorar esta característica son:[61] la estructura jerárquica de la organización, existencia de una cadena de mando, conjunto de reglas internas y símbolos externos de autoridad. Así como que las y los miembros del

---

[57] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Dario Kordic and Mario Cerkez. Sentencia de fondo de 17 de diciembre de 2004. Caso No. IT-95-14/2-A, párr. 341.

[58] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Fatmir Limaj, Haradin Bala, and Isak Musliu. Sentencia de fondo de 30 de noviembre de 2005. Caso No. IT-03-66-T, párr. 89.

[59] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Ljube Koskoski Johan Tarculovski. Sentencia de fondo de 10 de julio de 2008. Caso No. IT-04-82-T, párr. 177.

[60] *Ibidem*, párr. 178.

[61] *Ibidem*, párr. 195.

grupo se conduzcan conforme a los estándares del grupo y con sujeción a la autoridad de la o el jefe del grupo.

Lo anterior, no implica que los grupos armados organizados deban tener la misma organización que las fuerzas armadas de un Estado. Sin embargo, el grupo sí debe contar con algún grado de organización para que su participación configure la existencia de un conflicto armado.[62]

En ese sentido, se han identificado cinco grupos de factores que aportan indicios del grado de organización de un grupo armado:[63] presencia de una estructura de comando, capacidad de llevar a cabo operaciones de forma organizada, nivel de logística, capacidad de hablar con una sola voz, así como la disciplina y capacidad de implementar las obligaciones básicas del artículo 3 común a los cuatro "Convenios de Ginebra de 1949".

Por otro lado, el "Protocolo Adicional II a los Convenios de Ginebra", que también se aplica en el contexto de conflictos armados no internacionales, requiere un estándar más alto de organización. El grupo armado organizado debe tener un grado de estabilidad en el control de al menos un área del territorio en cuestión, lo que aseguraría la posibilidad de aplicar efectivamente las reglas del protocolo —artículo 1(1)—. Por ende, excluye grupos con poca incidencia en el territorio donde actúan.

Asimismo, la aplicación del "Protocolo Adicional II a los Convenios de Ginebra" únicamente se extiende a un conflicto entre fuerzas gubernamentales y

---

[62] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Naser Oric. Sentencia de fondo de 30 de junio de 2006. Caso No. IT-03-68-T, párr. 254.
[63] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Ljube Koskoski Johan Tarculovski, *Op. Cit.*, párrs. 199-203.

grupos armados organizados —artículo 1(1)—. Así, excluye conflictos en los que no se involucren las fuerzas del Estado, como enfrentamientos solamente entre grupos armados organizados.[64]

En relación con los conflictos armados no internacionales que no cubre el "Protocolo Adicional II a los Convenios de Ginebra", aún sería aplicable el artículo 3 común a los cuatro "Convenios de Ginebra" y los principios consuetudinarios del derecho internacional humanitario.

1.4. Objeto de regulación

El derecho internacional humanitario regula el uso de medios y métodos de guerra. En cuanto a los medios, implica la prohibición o regulación del desarrollo, posesión y uso de ciertas armas. En cuanto a los métodos, implica la prohibición o restricción de las formas en que determinadas armas pueden ser usadas o la manera en que las hostilidades pueden ser conducidas.[65]

En ese tenor, cualquier arma puede ser usada de forma ilícita si se emplea un método no permitido. Sin embargo, el uso de armas cuyo uso está prohibido por sus características inherentes, es ilícito sin importar la manera en que sean usadas.[66] En consecuencia, cobra relevancia abordar las razones de exclusión

[64] Cfr. SANDOZ, Yves, *et al.* (eds.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, S.N.E., Martinus Nijhoff Publishers, Ginebra, 1987, párr. 4461.
[65] Cfr. MELZER, Nils, International Humanitarian Law: A Comprehensive Introduction, S *Op. Cit.*, pág. 104.
[66] *Idem*.

de ciertos medios y métodos de guerra, que en general, servirán de base para la exclusión de nuevas armas o formas de conducir las hostilidades.

1.4.1. Medios

La prohibición de cierto tipo de armas se basa en el respeto al "Principio de evitar daño superfluo y sufrimiento innecesario".[67]

Sobre el particular, armas específicamente reguladas por el derecho internacional humanitario son:[68] veneno, balas explosivas o expansivas, fragmentos no detectables, trampas cazabobos y otros dispositivos controlados remotamente o por temporizador, minas terrestres, armas incendiarias, armas láser cegadoras, municiones de racimo, remanentes explosivos de la guerra, armas químicas, armas biológicas y armas nucleares.

Por otro lado, el derecho internacional humanitario prohíbe el uso de armas que por su naturaleza tengan efectos indiscriminados.[69] Asimismo, está prohibido el uso de armas que causen daños extensos, duraderos y severos al medio ambiente natural.[70]

---

[67] *Ibidem*, pág. 109.

[68] *Ibidem*, págs. 112-121.

[69] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 71, pág. 244.

[70] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, Guidelines on the protection of the natural environment in armed conflict: rules and recommendations relating to the protection of the natural environment under international humanitarian law, with commentary, ICRC, Ginebra, 2020, Regla 2, pág. 29; Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 45, pág. 151.

Finalmente, es notable mencionar que el artículo 36 del "Protocolo Adicional I a los Convenios de Ginebra" prevé 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 Parte contratante".

En ese tenor, el análisis de la legalidad de armas nuevas dependerá de su diseño y características inherentes, así como del lugar y forma en que se pretende usarlas.[71] Aunque este artículo está contenido en el "Protocolo Adicional I a los Convenios de Ginebra", todos los Estados deben realizar una revisión de todas las armas que utilicen, en función de evitar violaciones a los principios del derecho internacional humanitario.[72] Lo anterior, es particularmente cierto en función de los principios consuetudinarios que son vinculantes a todos los Estados.

1.4.2. Métodos

De conformidad con el "Protocolo Adicional I a los Convenios de Ginebra" y las normas consuetudinaria homólogas, las partes beligerantes deben abstenerse de

[71] Cfr. MELZER, Nils, International Humanitarian Law: A Comprehensive Introduction, *Op. Cit.*, pág. 123.
[72] *Ibidem*, pág. 122.

realizar ataques directos contra población o bienes civiles —artículo 48—,[73] propiedad cultural —artículo 53—,[74] u obras e instalaciones que contengan fuerzas peligrosas, lo que incluye presas, diques o centrales nucleares de energía eléctrica —artículo 51(4)—.[75] De igual forma, se prohíben los ataques indiscriminados —artículo 51(2)—,[76] como reflejo de la aplicación de los "Principios de Distinción y Precaución".

Igualmente, están prohibidos los actos o amenazas de violencia para aterrorizar a la población civil —artículo 51(2)—.[77] Así como, hacer padecer hambre a las personas civiles como método de guerra —artículo 54(1)—.[78]

Asimismo, se encuentra prohibida la conducción de la guerra que implique usar civiles —artículo 51(7)— u otras personas protegidas como escudos humanos;[79] o causar daños extensos, duraderos y graves al medio ambiente natural —artículos 35(3) y 55(1)—.[80]

Por otro lado, se prohíben los ataques a las personas que se encuentren fuera de combate u *hors de combat* por su nombre en francés —artículo 41(1)—.[81] Una persona fuera de combate, es aquella que está en poder del enemigo, es decir, bajo su control físico o territorial efectivo, que de forma clara expresa su

[73] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Reglas 1 y 7, págs. 3 y 25.
[74] *Ibidem*, Regla 38, pág. 127.
[75] *Ibidem*, Regla 48, pág. 139.
[76] *Ibidem*, Regla 11, pág. 37.
[77] *Ibidem*, Regla 2, pág. 8.
[78] *Ibidem*, Regla 53, pág. 186.
[79] *Ibidem* , Regla 97, pág. 337.
[80] *Ibidem*, Regla 45, pág. 151.
[81] *Ibidem*, Regla 47, pág. 164.

intención de rendirse o se encuentra incapaz de defenderse y que, en cualquier caso, se abstiene de todo acto hostil o intento de evadirse.[82]

En consonancia, se prohíbe la amenaza o real conducción de las hostilidades bajo la orden de negación de cuartel —artículo 40—,[83] *id est*, ordenar que no haya supervivientes.

Se prohíbe valerse de la perfidia para matar, herir o capturar a un adversario. La perfidia se constituye por aquellos actos que apelan a la buena fe de la parte contraria con la intención de traicionarla, por medio de hacer entender a esta última que está obligada a conceder protección —artículo 37(1)—.[84]

1.5. Conclusiones

De conformidad con lo expuesto en los apartados anteriores, se puede concluir que:

- El derecho internacional humanitario regula la conducción de las hostilidades en conflictos armados internacionales y no internacionales.
- El derecho internacional humanitario regula el uso de medios y métodos de guerra con base en los principios consuetudinarios del derecho internacional humanitario.

[82] Cfr. MELZER, Nils, International Humanitarian Law: A Comprehensive Introduction, *Op. Cit.*, pág. 106.
[83] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 46, pág. 161.
[84] *Ibidem*, Regla 65, pág. 221.

- No hay un marco de derecho internacional humanitario convencional que regule la ciberguerra.
- Únicamente se cuenta con ciertas provisiones que en general aplican a la conducción de las hostilidades mediante el uso del ciberespacio, tales como los artículos que codifican los principios reguladores del derecho internacional humanitario consuetudinario y el artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra” que regula el desarrollo y adquisición de armas nuevas.

Capítulo 2. Ciberguerra

El propósito de este capítulo es exponer qué se entiende por operaciones cibernéticas y los distintos tipos que hay, para posteriormente estudiarlos en el contexto de un conflicto armado y comprender qué se entiende por ciberguerra y su relación con el derecho internacional humanitario.

2.1. Ciberespacio

El término ciberespacio fue popularizado por el escritor William Gibson. Lo utilizó en una historia corta llamada *burning chrome* en 1982. Posteriormente, amplió la noción de ciberespacio en su novela *neuromancer* de 1984, en la que refirió que el ciberespacio era:[85]

> "Una alucinación consensual experimentada diariamente por billones de operadores legítimos, en todas las naciones, por niños a los que se les enseñan conceptos matemáticos (…) Una representación gráfica de datos abstraída de los bancos de todas las computadoras en el sistema humano. Complejidad impensable. Líneas de luz en el no-espacio de la mente, ramificaciones y constelaciones de datos. Como las luces de la ciudad, retrocediendo."

[85] BIGSON, William, "Neuromancer", citado por DELERUE, François, Cyber Operations and International Law, S.N.E., Cambridge University Press, Reino Unido, 2020, pág. 10: "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding".

Desde un aspecto técnico, recientemente el Departamento de Defensa de Estados Unidos definió el ciberespacio, en su diccionario de términos militares y asociados:[86]

> "Un dominio global dentro del entorno de la información que consiste en las redes interdependientes de infraestructuras de tecnología de la información y datos residentes, incluyendo internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados (…)"

El profesor Joseph Nye describe el ciberespacio en un contexto más político:[87]

> "El dominio cibernético incluye el Internet de computadoras interconectadas, pero también la intranet [redes de computadoras internas, no públicas como la Internet], las tecnologías celulares, los cables de fibra óptica y las comunicaciones basadas en el espacio. El ciberespacio tiene una capa de infraestructura física que sigue las leyes económicas de los recursos rivales y las leyes políticas de la justificación y el control soberanos."

---

[86] OFFICE OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF, DOD Dictionary of Military and Associated Terms, *Op. Cit.*, pág. 55: "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

[87] Cfr. NYE, Joseph, "The Future of Power", citado por VALERIANO, Brandon y MANESS, Ryan, Cyber War versus Cyber Realities: cyber conflict in the international system, S.N.E., Oxford University Press, Nueva York, 2015, pág. 22: "The cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign justification and control".

La doctrina también ha considerado que el ciberespacio es el entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos mediante redes informáticas.[88]

Una vez consideradas las definiciones anteriores, desde el origen literario del término hasta su concepción dentro de un contexto de seguridad nacional y de política, podemos colegir que el término ciberespacio, en esencia, se refiere el entorno formado por componentes físicos y no físicos que permiten el tráfico de información entre dispositivos interconectados en distintos niveles de alcance a través de redes informáticas.

Ahora bien, las operaciones que se van a describir a continuación se desarrollarán en el ciberespacio tal como se ha definido anteriormente.

2.2. Operaciones cibernéticas

Este apartado únicamente se abocará a la descripción del tipo de operaciones cibernéticas que hasta ahora se han llevado a cabo. Esto con la finalidad de discernir entre aquellas que pueden y deben ser materia de la aplicación de los principios del derecho internacional humanitario.

A las operaciones cibernéticas también se les conoce como operaciones de redes informáticas o *computer network operations* por su nombre en inglés. Este tipo de operaciones conlleva el empleo de capacidades del ciberespacio

[88] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, 2a ed., Cambridge University Press, Reino Unido, 2017, Glosario, pág. 564.

para alcanzar objetivos en o a través de este último.[89] Por ende, este trabajo se referirá a una operación cibernética, es decir, que utilice una red informática, sin que sea necesario que tenga lugar en el *internet* —red de redes que permite la comunicación entre otras redes y facilita operaciones remotas—.[90]

Cabe aclarar que, una red informática es "(…) un conjunto de dispositivos informáticos autónomos interconectados. Se dice que dos ordenadores están interconectados si pueden intercambiar información. La interconexión puede realizarse a través de diversos medios de transmisión, como el cable de cobre, el cable de fibra óptica y las ondas de radio (…)".[91]

Las acciones llevadas a cabo en el ciberespacio para obtener inteligencia, maniobrar, recopilar información o realizar otras acciones necesarias y prepararse para futuras operaciones militares se les conoce como *cyberspace exploitations*.[92] Es decir, tomar ventaja de los puntos endebles de los sistemas operativos: explotar sus fallas.

Las operaciones cibernéticas suelen aprovechar vulnerabilidades, es decir, la debilidad en los sistemas de seguridad. Por ejemplo, en 2017, el programa maligno *notpetya*, fue creado para atacar las vulnerabilidades en el sistema operativo *windows*. El programa podía extraer contraseñas y así ganar

---

[89] DELERUE, François, Cyber Operations and International Law, S.N.E., Cambridge University Press, Reino Unido, 2020, pág. 29.
[90] *Ibidem*, pág. 12.
[91] TANENBAUM, Andrew, FEAMSTER, Nick y WETHERALL, David, Computer Networks, 6a ed., Pearson Education Limited, Reino Unido, 2021, pág. 2: "a collection of interconnected, autonomous computing devices. Two computers are said to be interconnected if they can exchange information. Interconnection can take place over a variety of transmission media including copper wire, fiber optic cable, and radio waves…".
[92] OFFICE OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF, DOD Dictionary of Military and Associated Terms, *Op. Cit.*, pág. 55.

acceso a distintas funciones de los dispositivos infectados. *notpetya* se extendió rápidamente a bancos ucranianos, sistemas de pago, plantas de energía, hospitales, entre otros.[93]

Una operación cibernética puede diferenciarse en dos grandes momentos: preparación y ejecución. El conocimiento de la vulnerabilidad no implica su explotación inmediata. Incluso quien realiza la operación puede considerar conveniente no explotar dicha falla para no alertar al propietario del sistema informático. Así, la debilidad es aprovechada eventualmente cuando resulta más pertinente a quien pretende efectuar la operación. Es aquí en donde cobra relevancia la constante actualización de los mecanismos de seguridad y revisión del sistema.

Asimismo, cabe destacar la idea del *internet* de las cosas, que consiste en toda la constelación de objetos diseñados para conectarse entre sí a través del *internet*, lo que permite que puedan ser monitoreados, controlados y vinculados a través de la red. Estas capacidades se incluyen cada vez más en diversos objetos, lo que a su vez incrementa los posibles objetivos de operaciones cibernéticas.[94] Al respecto, el acceso a un sistema puede incluso generarse desde la lógica de más bajo nivel que controla los circuitos electrónicos del dispositivo; esto permitiría ganar un acceso de gran escala.[95]

---

[93] Cfr. SHACKELFORD, S., Douzet, F. y ANKERSEN, C. (eds.), Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace, S.N.E., Cambridge University Press, Estados Unidos, 2022, pág. 227.
[94] Cfr. SIMON, T. y la Comisión Global sobre Gobernanza de Internet, "*Critical infrastructure and the internet of things*", en Cyber Security in a Volatile World, 2017, pág. 97.
[95] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, S.N.E., ICRC, Ginebra, 2019, pág. 24.

En general, las operaciones cibernéticas quedan comprendidas en el modelo de cadena mortal o *kill chain model*, por su nombre en inglés. El modelo consta de 7 pasos: 1) reconocimiento, 2) armamento, 3) entrega, 4) explotación, 5) instalación, 6) comando y control, y 7) acciones y objetivos.[96]

El reconocimiento implica investigar, identificar y seleccionar objetivos. La etapa de armamento conlleva alistar el programa que permitirá explotar debilidades del sistema objetivo para establecer una conexión remota. El paso de entrega consiste en transmitir el programa previamente referido, que puede ser a través de correos, sitios *web* o dispositivos USB.[97]

Una vez que el programa fue entregado, sigue la explotación, es decir, se activa el programa que aprovechará las debilidades del sistema, y el programa instala un acceso permanente en el objetivo. De esta forma, un servidor externo puede establecer comando y control sobre el sistema afectado. Esto permite que el invasor pueda realizar las acciones para alcanzar su propósito.[98]

En este orden de ideas, es notable mencionar que hay actores que realizan operaciones cibernéticas mediante el uso de grandes capacidades y con objetivos muy concretos. En otras palabras, son personas que usualmente están financiadas por gobiernos o entidades no estatales con muchos recursos y que buscan algo más que una ganancia económica. A estos agentes se les conoce

[96] Cfr. DALZIEL, H., Securing Social Media in the Enterprise, S.N.E., Syngress, Estados Unidos, 2015, pág. 7.
[97] Cfr. BERGH, A., "*Understanding Influence Operations in Social Media: A cyber Kill Chain Approach*", en Journal of Information Warfare, Vol. 19(4), 2020, pág. 112.
[98] *Idem*.

como amenaza persistente avanzada o *advanced persistent threat* por su nombre en inglés.[99]

Ahora bien, las operaciones cibernéticas pueden causar o no efectos físicos. Algunas operaciones se llevan a cabo únicamente para obtener información, mientras que otras buscan afectar el dispositivo que contiene la información relevante. A continuación, se describen estos dos tipos de operaciones.

2.2.1. Operaciones cibernéticas con efectos cinéticos

Las operaciones cibernéticas con efectos cinéticos tienen consecuencias en el mundo físico, ya sea directa o indirectamente, y causan daño, lesiones o la muerte. Esto únicamente a través de la explotación de vulnerabilidades en los procesos y sistemas de información. Este tipo de operaciones se llevan a cabo sobre sistemas ciber-físicos, es decir, aquellos que coordinan los recursos informáticos y los físicos.[100]

Por ejemplo, este tipo de sistemas se han integrado a dispositivos médicos, control del tráfico y seguridad, sistemas automotores avanzados, controladores de procesos, conservación de energía, control medio ambiental, aviónica, instrumentación, control de infraestructuras críticas como energía

[99] Cfr. CUNNINGHAM, Chase, Cyber Warfare – Truth, Tactics, and Strategies, S.N.E., Packt Publishing, Reino Unido, 2020, págs. 24-25.
[100] Cfr. APPLEGATE, Scott, “The Dawn of Kinetic Cyber”, en PODINS, K., STINISSEN, J. y MAYBAUM, M.(eds.), 5th International Conference on Cyber Conflict, Tallin, 2013, pág. 1.

eléctrica, recursos hídricos y sistemas de comunicación, robótica, sistemas de defensa, procesos de manufacturación y estructuras inteligentes.[101]

A este tipo de operaciones se les conoce como ataque a red informática o c*omputer network attack* por su nombre en inglés. Estas operaciones cibernéticas pretenden causar un perjuicio a la información que contienen ordenadores y redes informáticas, o pretenden destruir los ordenadores y redes en sí mismas. Los efectos de las operaciones de ataque a redes informáticas suelen ser de 5 tipos:[102] 1) engaño, 2) interrupción, 3) negación, 4) degradación y 5) destrucción.

El engaño se relaciona con la manipulación de los sistemas de comunicación, con el propósito de falsificar el intercambio de información, alterar su tránsito o simplemente desaparecer el tráfico de datos.

La interrupción se asocia con los procesos, recursos, archivos y cualquier tarea que pueda ser alterada.

La negación implica hacer fallar algún servidor donde el público accede y así detener su funcionamiento, por ejemplo, servidores *web* o de correo electrónico.

La degradación conlleva perjudicar el rendimiento de algún sistema o red informática, de tal forma que falle en su funcionamiento y de forma esporádica, por ejemplo, al alterar la manera en que opera un sistema que procesa información para que produzca datos incorrectos.

---

[101] *Idem.*

[102] Cfr. ANDRESS, J. y WINTERFELD, S., Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 2a ed., Syngress, Estados Unidos, 2014, págs. 181 y 189.

La destrucción cubre varias acciones como causar estragos en información, aplicaciones o sistemas operativos; incluso cubre intentos de provocar daño físico al dispositivo en el que trabaja el sistema operativo.[103]

Si algo utiliza procesos computacionales para funcionar, como armas o sistemas de armas, entonces es vulnerable a ser desactivado si se consigue acceso a dichos sistemas.[104]

Por ejemplo, Israel llevó a cabo una operación cibernética para infiltrarse en el sistema de defensa aérea de Siria en 2007. Esta operación no dañó el sistema, sino que cargó información falsa para que éste no alertara la aparición de posibles amenazas en el espacio aéreo. Luego de manipular este sistema, Israel condujo un ataque aéreo en la infraestructura de Siria.[105]

Asimismo, se pueden llevar a cabo operaciones que interfieran con la funcionalidad de los dispositivos o sistemas objetivo a tal punto que se requiera el reemplazo físico del dispositivo o sistema en su totalidad o de algunos de sus componentes. *V.gr.*, una operación dirigida a detener el funcionamiento de una red de distribución eléctrica operada por un sistema de control por ordenador.[106]

En ese sentido, los efectos de una operación cibernética pueden generar la necesidad de reinstalar el sistema operativo o algunos datos en particular, en

---

[103] Cfr. *Ibidem*, pág. 190.

[104] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, págs. 30 y 35.

[105] Cfr. POOL, Phillip, "*War of the Cyber World: The Law of Cyber Warfare*", en The International Lawyer, American Bar Association, Estados Unidos, Vol. 47, Núm. 2, 2013, pág. 304.

[106] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 92, pág. 417, párr. 10.

función de poner nuevamente en operación la ciber infraestructura afectada y que cumpla el propósito para el que fue diseñado.[107]

Un ejemplo es el programa maligno *stuxnet*, descubierto en 2010 en Irán. Este programa se diseñó para sabotear las operaciones de equipamiento industrial utilizado en redes eléctricas, plantas de energía, tuberías y presas. *Stuxnet* tuvo impacto en más de 100,000 computadoras, donde el 60% se localizaban en Irán. En particular, afectó el correcto funcionamiento de plantas de uranio de ese país.[108]

Por otro lado, hay operaciones que pueden variar de objetivo según el programa utilizado y su función, pues una vez que se accede a un dispositivo se pueden realizar diversas acciones. Por ejemplo, robar información o controlar un dispositivo remotamente para llevar a cabo una operación de denegación de servicio distribuido o d*istributed denial of service,* por su nombre en inglés. A estos dispositivos controlados de forma remota se les conoce como *botnets*.[109]

Estas operaciones, que impiden el uso de un servicio, sobrepasan la capacidad de los servidores a través de una constante visita realizada por los dispositivos controlados. Como resultado, el sistema en cuestión funciona incorrectamente.[110]

---

[107] *Ibidem*, Regla 92, pág. 417, párr. 11.
[108] Cfr. HAATAJA Samuli y AKHTAR-KHAVARI, Afshin, "*Stuxnet and International Law on the Use of Force: an International Approach*", en Cambridge International Law Journal, Vol. 7, 2018, pág. 101.
[109] Cfr. HATHAWAY, Oona, *et al.*, "*The Law of Cyber-Attack*", en California Law Review, California Law Review Inc., Estados Unidos, Vol. 100, Núm. 4, 2012, pág. 837.
[110] *Idem*.

Las operaciones cibernéticas de denegación de servicio distribuido pueden ocurrir de dos formas: a nivel de red, cuando se ataca la infraestructura del *internet* al mandar un gran número de paquetes de datos, y a nivel de aplicación, cuando se dirige a servicios específicos o componentes de un sitio *web*, posiblemente basado en su diseño.[111]

Un *botnet* se crea a partir de un programa instalado en un dispositivo, mismo que le permite al atacante tener control remoto del objetivo infectado. La forma más común de controlar el funcionamiento de una red de *botnets* es a través del chat de retransmisión por internet o *internet relay Chat*, por su nombre en inglés, que es un sistema que permite intercambiar mensajes de texto. La persona que realiza la operación establece un servidor de chat de retransmisión por *internet* y abre un canal de comunicación específico donde comparte sus comandos. Los *botnets* se conectan a este chat y actúan bajo los comandos que reciben por este medio.[112]

El servidor que emite los comandos se conoce como servidor de mando y control o *command and control server,* por su nombre en inglés. Este servidor de mando y control también puede ser establecido en un servidor *web* al que se conectan los *botnets* para recibir instrucciones. Por ejemplo, se pueden conectar

[111] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, págs. 29-30.
[112] Cfr. HOLZ, Thorsten, *et al.*, "*Measures and Mitigation of Peer-to-Peer-based Botnets: A case Study on Storm Worm*", en Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Trheats, Estados Unidos, Núm. 9, 2008, pág. 1.

al servidor *web* para descargar un archivo con las instrucciones que deben seguir.[113]

Actualmente, los *botnets* pueden trabajar de otra forma: comunicación por pares o *peer-to-peer,* por su nombre en inglés. En este caso, los *botnets* no tienen un servidor central que distribuya los comandos, como en el caso de la comunicación chat de retransmisión por *internet*. Esto dificulta rastrear el origen de los comandos que reciben los *botnets*.[114]

Por ejemplo, el programa maligno *storm worm* funcionaba con el sistema de comunicación por pares. El *botnet* se distribuyó a través de correos electrónicos que contenían información sobre noticias actuales o felicitaciones por alguna celebración festiva. El programa obtenía acceso a los dispositivos a través de la participación de las víctimas cuando entraban al contenido del correo.[115]

Adicionalmente, el sistema de comunicación por pares permitía que cada dispositivo parte de la red de *botnets* funcionara como canal de comunicación. Esto en conjunto con la técnica *fast-flux*, que cambia los registros de los nombres de los servidores cada 3 o 10 minutos. De tal forma que, cada vez que se establecía comunicación, se hacía a través de una dirección IP distinta y con mensajes encriptados.[116]

---

[113] Cfr. MARYLISE, Nellly, Storm Worm: A P2P Botnet, S.N.E., Norwegian University of Science and Technology, Noruega, 2008, págs. 5 y 7.
[114] Cfr. HOLZ, Thorsten, *et al.*, "*Measures and Mitigation of Peer-to-Peer-based Botnets: A case Study on Storm Worm*", *Op. Cit.*, pág. 1.
[115] Cfr. MARYLISE, Nellly, Storm Worm: A P2P Botnet, *Op. Cit.*, págs. 2, 9-10.
[116] *Ibidem*, págs. 7-8, 10 y 12.

Por otro lado, el *blackenergy* es un programa malicioso hecho para afectar plantas eléctricas. Este programa es tan versátil que es utilizado para iniciar diversas modalidades de ataque, entre ellas, denegación de servicio distribuido o directamente dejar inservible el sistema. Este programa ha evolucionado a lo largo de los años y es utilizado en distintas operaciones. En 2015, se utilizó para dejar sin energía eléctrica a una región de Ucrania durante 6 horas aproximadamente.[117]

En la misma línea de programas que causan la pérdida de funcionamiento, uno de los ejemplos más famosos es el programa *wannacry*, utilizado en 2017. Este programa tenía la capacidad de escanear y localizar otras computadoras para propagarse automáticamente.[118] *wannacry* es un *ransomware*, es decir, es un programa que bloquea el acceso de usuarios a archivos, sistemas, o dispositivos. El bloqueo únicamente se remueve cuando la víctima paga el rescate que exige el agente que utiliza el programa.[119]

El ataque de *wannacry* afectó alrededor de 200,000 computadoras de más de 150 países. El sector médico británico fue el más afectado: el *ransomware* impactó el Servicio Médico Nacional de Inglaterra. El personal médico no pudo

---

[117] Cfr. EASTTOM, C., "*An Examination of the Operational Requirements of Weaponised Malware*", en Journal of Information Warfare, Peregrine Technical Solutions, Estados Unidos, Vol. 17, Núm. 2, 2018, pág. 3; KHAN, R, *et al.*, "*Threat Analysis of BlackEnergy for Synchrophasor based Real-timeControl and Monitoring in Smart Grid*", en 4th International Symposium for ICS & SCADA Cyber Security Research, 23-25 agosto de 2016, pág. 3.

[118] Cfr. HARKINS, M. y FREED, A., "*The Ransomware Assault on the Healthcare Sector*", en Journal of Law & Cyber Warfare, Lexeprint, Inc, Estados Unidos, Vol. 6(2), 2018, págs. 158-159.

[119] Cfr. MOHURLE, S. y PATIL, M., "*A brief study of Wannacry Threat: Ransomware Attack 2017*", en International Journal of Advanced Research in Computer Science, Vol. 8, Núm. 5, 2017, pág. 1938.

acceder al historial de los pacientes, ni al equipo médico que fue bloqueado. En consecuencia, citas y procedimientos fueron cancelados.[120]

El sector médico también puede ser afectado de otras formas como implantes médicos que son colocados quirúrgicamente, que es el caso de marcapasos o bombas de insulina, que son vulnerables a ser controlados remotamente por terceros. La manipulación de estos dispositivos puede ocasionar la muerte de las personas afectadas.[121]

Así, podemos diferenciar la letalidad de los efectos de los distintos tipos de operaciones cibernéticas en contra del sector médico. Hasta ahora ha quedado claro que los perjuicios pueden ser de dos tipos: 1) efectos sobre dispositivos que almacenan información como historial o citas médicas; y, 2) dispositivos implantados quirúrgicamente, que son un insumo vital para quienes los tienen.

Claramente el segundo tipo de operación es más dañina e inmediata que la primera. Aunque los efectos causados por el primer tipo de operación también pueden resultar en grandes perjuicios.

Otro ejemplo de programa maligno es el vpn *filter*, creado para tener efectos sobre los enrutadores y propagarse a gran escala. En 2018, se identificaron 500,000 enrutadores afectados en 54 países. Este programa permite

---

[120] Cfr. MILANOVIC, M. y SCHMITT, M., "*Cyber Attacks and Cyber (Mis) information Operations During a Pandemic*", en Journal of National Security and Law & Policy, Estados Unidos, Vol. 11, 2020, pág. 257

[121] Cfr. BRANTLY, A., "*The Violence of Hacking: State Violence and Cyberspace*", en The Cyber Defence Review, Army Cyber Institute, Estados Unidos, Vol. 2, Núm. 1, 2017, pág. 85; GUNNERIUSSON, H. y OTTIS, R, "*Cyberspace from the Hybrid Threat Perspective*", en Journal of Information Warfare, Peregrine Technical Solutions, Estados Unidos, Vol. 12, Núm. 3, 2013, pág. 73.

a su operador controlar todo el tráfico de información en los dispositivos afectados, recolectar y eliminar información, así como controlarlos remotamente y dejarlos fuera de servicio.[122] Luego de que las operaciones de este programa fueran desmanteladas, surgió el *cyclops blink*, con características similares. [123]

Las industrias también se han visto afectadas. El programa *triton* o *trisis* o *hatman*. fue diseñado para interactuar con los controladores de los Sistemas Instrumentados de Seguridad *triconex*, que son comúnmente utilizados para garantizar la operación segura de miles de plantas de infraestructura crítica alrededor de todo el mundo —plantas nucleares, químicas, de agua, de gas y de petróleo—. Este programa maligno fue detectado en 2017, en una planta química en Arabia Saudita. *triton* tiene la capacidad de destruir información y detener las operaciones de la planta en la que se infiltra.[124]

En agosto de 2012, el programa maligno *shamoon*, afectó aproximadamente 30,000 computadoras de la compañía petrolera *Saudi Aramco*. Alteró los archivos de la empresa y eliminó la información que permitía iniciar el sistema operativo de las computadoras. El objetivo de este programa era hacer que los sistemas de información de la compañía quedaran inservibles.[125]

---

[122] Cfr. MALIARCHUK, Tamara, "*Hybrid Warfare and Cyber Effects in Energy Infrastructure*", en *Connections*, Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Alemania, Vol. 18, Núm. 1, 2019, pág. 108.

[123] Cfr. NATIONAL CYBER SECURITY CENTRE, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, "New Sandworm malware Cyclops Blink replaces VPNFilter, Versión 1.0", Reino Unido, 2022, pág. 5.

[124] Cfr. EFRONY, Dan y SHANY, Yuval, "*A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*", en The American Journal of International Law, Cambridge University Press, Estados Unidos, Vol. 112, Núm. 4, 2018, pág. 622.

[125] Cfr. MELE, S., "*Legal Considerations on Cyber-Weapons and Their Definition*", en Journal of Law & Cyber Warfare, Lexeprint, Vol. 3, Núm. 1, 2014, pág. 62.

Con lo anterior, es posible observar que, los alcances de las operaciones cibernéticas de ataque a redes informáticas pueden tener efectos muy variados y en distintos sectores. Igualmente, los niveles de perjuicio que generan dependen del programa, el sector objetivo y las intenciones del agente que realiza la operación.

En el siguiente apartado se abordarán los efectos que pueden causar las operaciones que no tienen efectos cinéticos.

2.2.2. Operaciones cibernéticas sin efectos cinéticos

En contraste con las operaciones cibernéticas con efectos cinéticos, las que carecen de éstos son aquellas operaciones que únicamente afectan el ciberespacio, sin proyectarse al mundo físico.

Dentro de este tipo de operaciones se encuadran las de reconocimiento, vigilancia y extracción de datos o información. Este tipo de operaciones se conocen como explotación de redes informáticas o *computer network exploitation*, por su nombre en inglés. El objetivo de las operaciones de explotación de redes informáticas se deslinda de la potencial creación de daño al sistema:[126] entre menos sea detectada la actividad, mejor se podrá llevar a cabo la recolección de información. Sin embargo, una operación de explotación de redes informáticas puede progresar a una de ataque a redes informáticas.[127]

[126] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 12.
[127] Cfr. LIBICKI, Martin, Cyberdeterrence and Cyberwar, S.N.E., RAND Corporation, Estados Unidos, 2009, pág. 15.

Una operación de explotación de redes informáticas tuvo lugar en 1994, cuando dos piratas informáticos ingresaron a uno de los sistemas más clasificados de la Fuerza Aérea estadounidense: la red de Laboratorios de Roma.[128]

Otro ejemplo, es el programa malicioso *flame* que fue diseñado para infiltrarse y espiar en computadoras y sus sistemas a lo largo del Medio Oriente. Este programa era capaz de realizar diversas actividades de forma remota, como tomar capturas de pantalla, registrar las pulsaciones de las teclas y grabar audio, así como eliminar datos. *flame* afectó principalmente a Irán.[129]

Hasta este punto se han descrito operaciones cibernéticas independientemente del contexto. A continuación, se examinarán operaciones que pueden tener un impacto directo en conflictos armados.

2.3. Ciberguerra

Todo lo descrito en el apartado anterior sobre operaciones cibernéticas se describió sin tener en consideración un contexto en particular, pues podrían llevarse a cabo tanto en tiempo de paz como en tiempo de guerra. Ahora, se abordarán ejemplos específicos sobre los usos que se le puede dar a este tipo de operaciones en conexión con la conducción de las hostilidades.

[128] Cfr. SPRINGER, Paul J., Cyber Warfare, S.N.E., ABC-CLIO, Reino Unido, 2015, pág. 19.
[129] Cfr. ATREWS, R., "*Cyberwarfare*", en Journal of Information Warfare, Peregrine Technical Solutions, Estados Unidos, Vol. 19, Núm. 4, 2020, pág. 19.

Se analizarán las operaciones cibernéticas independientemente de si el conflicto se libra en el ciberespacio o en compañía de operaciones físicas en dominios como el terrestre, aéreo, marítimo o espacio exterior.

Asimismo, es importante describir el papel que las operaciones cibernéticas pueden jugar dentro de un conflicto armado. A este respecto, resulta útil considerar la definición de conflicto armado que se presentó en el capítulo anterior en torno al derecho internacional humanitario, es decir: en su carácter internacional, "(…) existe un conflicto armado cuando se recurre a la fuerza armada entre Estados (…)"[130] o un conflicto armado no internacional cuando hay "(…) violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre tales grupos dentro de un Estado".[131]

En ese tenor, cabe diferenciar dos momentos en los que el uso de medios o métodos de guerra tienen relevancia en el contexto de un conflicto armado: el uso de capacidades cibernéticas puede aparecer como detonante de un conflicto armado en cualquiera de sus caracterizaciones; o bien, estas capacidades pueden emplearse una vez que el conflicto ya existe.

En consonancia con lo anterior, es importante resaltar que en el primer supuesto la operación cibernética empleada tendría que cubrir con las características de un ataque, en función de alcanzar el nivel de violencia o fuerza empleada como detonante de un conflicto armado. En cambio, bajo el segundo

[130] TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Dusko Tadic, *Op. Cit.*, párr. 70: "…an armed conflict exists whenever there is a resort to armed force between States…".
[131] *Idem*: "…protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".

supuesto, no es necesario que las operaciones cibernéticas en cuestión cumplan con determinado umbral de violencia o efectos; basta con emplearlas dentro del contexto del conflicto y en conexión con éste.

En ese sentido, este trabajo únicamente se avocará al estudio de las operaciones cibernéticas como medios o métodos de guerra y no como detonantes de un conflicto armado.

Es relevante definir qué se entiende por ciberguerra, en función de no confundir este concepto con un conflicto armado. Así, podemos entender la ciberguerra "como las acciones de los Estados-nación para penetrar en los ordenadores o redes de otra nación con el fin de causar daños o disrupciones".[132] Aunque esta descripción se circunscribe a considerar actores estatales, en la realidad son más los actores no estatales quienes desarrollan actividades en el ciberespacio. No obstante, en ocasiones puede que las actividades de estos actores no estatales estén motivadas y sufragadas por el Estado.

La definición antes prevista sobre ciberguerra es relevante en función de que el término se emplea únicamente para referir el recurso a operaciones cibernéticas con el propósito de causar efectos adversos, independientemente del contexto de un conflicto armado. Sin embargo, es preciso conceptualizar el término en el entorno que nos ocupa.

[132] CLARKE, Richard y KNAKE, Robert, "Cyber War: The Next Threat to National Security and What to Do About It", citado por VALERIANO, Brandon y MANESS, Ryan, Cyber War versus Cyber Realities: cyber conflict in the international system, S.N.E., Oxford University Press, Nueva York, 2015, pág. 29: "as actions by nation-states to penetrate another nation's computers or networks for the purposes of causing damage or disruption".

En ese tenor, el Comité Internacional de la Cruz Roja entiende la guerra cibernética como "las operaciones lanzadas contra un ordenador o un sistema de ordenadores a través de una corriente de datos, cuando se usan como medios y métodos de guerra en el contexto de un conflicto armado según se encuentra definido en el derecho internacional humanitario."[133]

Cabe resaltar que, una operación cibernética no constituirá un ataque cibernético necesariamente. Un ataque cibernético se puede entender en sentido amplio como "(…) cualquier operación cibernética llevada a cabo sin el consentimiento o conocimiento del propietario del sistema objetivo, para obtener acceso, extraer información y/o encriptarla, degradarla, borrarla, modificarla o deshabilitar información o servicios".[134]

Sin embargo, una definición más apropiada debería coincidir con la delimitación que contempla el artículo 49(1) del "Protocolo Adicional I a los Convenios de Ginebra" respecto de qué se entiende por ataque, es decir: actos de violencia contra el adversario, sean ofensivos o defensivos.

En ese sentido, cualquier acto de violencia se configura como ataque, ya sea de pequeña o gran escala. La violencia se entiende en los términos de las consecuencias, más que en el acto en sí mismo. De esta suerte, actos violentos incluyen ataques cibernéticos que provoquen efectos violentos.[135]

---

[133] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, "El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos", Documento 32IC/15/11, Ginebra, Suiza, 8-10 de diciembre de 2015, pág. 51.

[134] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 11: "…any cyber operation carried out without the consent or knowledge of the owner of the targeted system, to obtain access, extract data and/or encrypt, degrade, delete, modify or disable data or services".

[135] Cfr. DINSTEIN, Yoram, The Conduct of Hostilities under the Law of International Armed Conflict, S.N.E., Cambridge University Press, Nueva York, 2004, pág. 84.

Es decir, un ataque cibernético es la operación que utiliza medios cibernéticos con el propósito de causar un perjuicio a una computadora, a un sistema de computadoras o a la información que contienen.[136]

En la doctrina, el "Manual de Tallinn 2.0" sobre la aplicación del derecho internacional aplicable a la ciberguerra, sugiere que "un ataque cibernético es una operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente que cause lesiones o muerte a personas o daños o destrucción de objetos".[137]

Al respecto, podemos resaltar una operación cibernética como el espionaje u operaciones psicológicas a través del ciberespacio. Estas actividades no conllevan efectos violentos en sí mismas, por ende, no califican como ataque. En contraste, una operación que tenga por objetivo dañar un sistema de control industrial sí califica como ataque independientemente de que surta efectos o no, incluso en caso de no producir todos los efectos deseados se constituiría como el intento de un ataque. Esto es debido a que pudo causar efectos violentos.[138]

Esto se clarifica si revisamos el siguiente ejemplo: si un militar dispara hacia un combatiente de las fuerzas enemigas, esto constituye un ataque, pues pretende causar efectos violentos sobre la parte beligerante contraria; sin embargo, el disparo no necesariamente causará la baja de la víctima, o incluso

---

[136] Cfr. CHAYES, A., Borderless Wars: Civil Military Disorder and Legal Uncertainty, S.N.E., Cambridge University Press, Estados Unidos, 2015, págs. 135-136.

[137] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 92, pág. 415: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".

[138] *Ibidem*, Regla 92, pág. 415, párrs 2 y 3

no necesariamente será impactada por el disparo. Aun así, no hay duda de que ese disparo constituye un ataque.

Por otro lado, si bien una operación cibernética no siempre se relaciona con un ataque cibernético, sí es necesario discernir en qué momento se considera el empleo de capacidades cibernéticas como medio o como método de hacer la guerra.

En el capítulo anterior, se describió cuándo se utilizan los términos medios o métodos. En el caso de los primeros, son armas; mientras que los segundos son formas de usar un arma o de conducir las hostilidades. Ahora, cobra relevancia abordar qué tipo de operaciones cibernéticas encajan en qué categoría y en qué momento, en torno a los conflictos armados.

Es necesario aplicar el significado de medio y método de guerra a las operaciones cibernéticas antes descritas, pues derivado de esta clasificación será posible aplicar el derecho internacional humanitario de forma clara.

Sin perjuicio de lo anterior, es pertinente señalar que en muchas ocasiones encontraremos interrelacionada la utilización de un medio con un método de guerra cibernética. Esto deriva de la propia definición que se estableció de ambos en el capítulo anterior, ya que un método de guerra puede implicar la forma en que se utiliza un medio. Aun así, es pertinente marcar la distinción para discernir claramente las características de un medio y un método de guerra cibernética, lo que se aborda en las secciones subsecuentes.

Otra consideración relevante es que, debido a la naturaleza de las operaciones cibernéticas, éstas pueden realizarse desde un lugar remoto al espacio donde tiene lugar el conflicto armado en cuestión. A pesar de esto, las

operaciones cibernéticas todavía son reguladas por las leyes de la guerra, al menos en tanto que tienen conexión con el conflicto. En ese sentido, el criterio relevante recae en los efectos de las operaciones, ya sea sobre objetos o individuos.[139]

En el caso "*Kuranac*" *y otros,* el Tribunal Penal Internacional para la Antigua Yugoslavia analizó la aplicación del derecho internacional humanitario en función de la distancia entre los actos y el conflicto. El Tribunal refirió que, el requisito de que los actos deban estar "estrechamente relacionados" al conflicto armado no sería afectado si éstos estuvieron temporal y geográficamente alejados del lugar en el que realmente tuvo lugar el enfrentamiento. Añadió que, por ejemplo, sería suficiente que los actos estuvieran estrechamente relacionados con las hostilidades que ocurren en otras partes del territorio controlado por las partes en conflicto.[140]

En el caso mencionado, el Tribunal analizó una situación que tuvo lugar fuera del espacio estrictamente definido como el lugar donde ocurre el enfrentamiento. Sin embargo, todavía considera que los actos tienen lugar dentro del territorio controlado por alguna de las partes en el conflicto. Esto difiere de un caso hipotético en el que, por ejemplo, alguien podría realizar una operación cibernética en el territorio controlado por un Estado que no forma parte del conflicto.

---

[139] Cfr. HARRISON DINNISS, Heather, Cyber Warfare and the Laws of War, S.N.E., Cambridge University Press, Reino Unido, 2012, pág. 135.

[140] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, Prosecutor vs. Dragoljub Kunarac, Radomir Kovac y Zoran Vukovic. Sentencia de fondo de 12 de junio de 2002. Caso No. IT-96-23 & IT-96-23/1-A, párr. 57.

Sin embargo, en este último caso podría resultar útil transpolar la aplicación del mismo estándar de estrechamente relacionado, para determinar que un acto realizado fuera del territorio controlado por los oponentes en el conflicto armado está gobernado por el derecho de la guerra. Esto con la finalidad de que las partes beligerantes no se deslinden del gobierno del derecho internacional humanitario, sólo por no encontrarse en el territorio controlado por las partes en el conflicto.

Para tal efecto, puede considerarse: 1) que el actor sea un combatiente, 2) que la víctima sea o no combatiente, 3) que la víctima sea de la parte contraria en el conflicto, 4) que el acto sirva al propósito de una campaña militar y, 5) que el acto sea realizado en el contexto de los deberes oficiales del actor.[141]

Aunque el estándar y criterios antes fijados se desarrollaron en el marco de un caso que pretendía establecer responsabilidad penal individual, estos elementos son útiles para establecer la conexión de un acto y un conflicto armado. Esto es así porque, independientemente de la comisión de un crimen de guerra que implique la responsabilidad del actor, estos componentes pueden constituir partes objetivas en una evaluación de la conexión entre una operación cibernética y un conflicto armado.

2.3.1. Operaciones cibernéticas como medio de guerra

[141] *Ibidem*, párr. 59.

Los medios de guerra cibernéticos se constituyen por las armas cibernéticas o los sistemas asociados a estas últimas.[142] En ese tenor, las armas cibernéticas son "códigos computacionales que se utilizan, o están diseñados para ser utilizados, con el objetivo de amenazar o causar daños físicos, funcionales o mentales a estructuras, sistemas o seres vivos".[143]

Otra definición desarrollada específicamente en el contexto de ciberguerra conceptualiza un arma cibernética como la que se diseña para usarse en actividades que causarán lesiones o muerte a personas o que causarán daño o destrucción a objetos. Es decir, un arma cibernética es la que puede emplearse para efectuar un ataque. Por lo tanto, incluye dispositivos, materiales, instrumentos, mecanismos, equipamiento o programas diseñados para realizar un ataque cibernético. En este punto es relevante distinguir los sistemas computacionales que pueden utilizarse como armas y la infraestructura cibernética, *v.gr.* el *internet*. Esta última es sólo el medio por el que se lleva a cabo el ataque con el sistema computacional.[144] La ciber infraestructura se compone de los dispositivos de comunicación, almacenamiento y computación sobre los que se construyen y funcionan los sistemas de información.[145]

---

[142] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 103(a), pág. 452.
[143] RID, Thomas y McBURNEY, Peter, "Cyber Weapons", citado por VALERIANO, Brandon y MANESS, Ryan, Cyber War versus Cyber Realities, 2015, pág. 33.: "…computer codes that are used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings".
[144] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 103, pág. 452, párrs. 2-3.
[145] *Ibidem*, Glosario, pág. 564.

Igualmente, podemos distinguir los diversos efectos que puede provocar un ataque. En cuanto a los efectos sobre un sistema de control industrial, podemos considerar como posible objetivo una red eléctrica o una presa. Al respecto, es importante distinguir sobre quién o qué recae el efecto violento:[146] Por un lado, el efecto buscado puede recaer sobre un daño a la infraestructura; por otro lado, las consecuencias violentas pueden resultar más bien por la manipulación del sistema, sin que esto implique necesariamente que el sistema en sí mismo resulte dañado.

Ocurre lo mismo cuando hablamos de una operación cibernética cuyo objetivo se centra en un ataque sobre los datos de un sistema computacional. Se puede causar perjuicio a individuos u objetos.[147]

En otro orden de ideas, una operación cibernética puede combinarse con una operación tradicional como parte integral de una operación que constituye un ataque.[148] Por ejemplo, la operación cibernética descrita previamente en la que se neutralizó el sistema de defensa aérea de Siria en 2007, para realizar un ataque aéreo efectivo.

En este caso nos encontramos frente a un medio, que es el instrumento utilizado para desactivar el sistema, y un método de guerra cibernética, que es la estrategia de emplear el instrumento para deshabilitar el sistema. Este medio y método no conllevan a las consecuencias violentas por sí mismos. Las

[146] *Ibidem*, Regla 92, pág. 416, párrs. 3 y 5.
[147] *Ibidem*, Regla 92, págs. 416-417, párrs. 6 y 11.
[148] Cfr. HARRISON DINNISS, Heather, Cyber Warfare and the Laws of War, *Op. Cit.*, pág. 134.

consecuencias violentas surgen cuando la operación militar tradicional se lleva a cabo.

Sobre el particular, podemos distinguir dos momentos en la operación general: 1) operación cibernética; 2) operación tradicional. El acto violento nace de la segunda sub-operación, sin embargo, dentro de la operación general se incluye llevar a cabo la sub-operación uno. De tal suerte que, en la estrategia integral, no se realizaría la segunda sub-operación sin primero realizar la sub-operación uno.

Consecuentemente, a pesar de que la sub-operación uno no tiene efectos violentos, la interdependencia entre ésta y la segunda implica que la caracterización como ataque recaiga a la operación integral, *id est*, desactivar el sistema de defensa es un ataque en tanto que no se realizaría individualmente, pues se espera tomar ventaja de sus efectos para realizar la sub-operación dos.

Por otro lado, si se lleva a cabo la sub-operación uno individualmente, entonces no es un ataque. Luego, puede que haber desactivado el sistema se valore como una oportunidad que debe aprovecharse para infligir daño a la parte enemiga y, por ende, se efectúe una operación consistente en la sub-operación dos. En este caso, estamos frente a dos momentos claramente diferenciados en los que la segunda operación no fue planeada con dependencia de la primera operación. Por lo tanto, la primera operación no sería un ataque.

Vale la pena tomar en consideración cuáles son los usos que las partes beligerantes dan a los medios cibernéticos, es decir, no sólo la forma de llevar a cabo operaciones cibernéticas de ataque o defensa; sino que, detallar en qué se emplean los sistemas computacionales que podrían llegar a verse afectados.

Por ejemplo, si un *botnet* —dispositivo controlado por un programa maligno de forma remota— se esparce y gana control sobre dispositivos relevantes utilizados en operaciones militares específicas por una parte beligerante. En principio, la operación podría ser legítima, pero al ser un *botnet*, se podría propagar ilimitadamente y sin distinguir objetivos, según su configuración inicial.

Igualmente, un gusano o un troyano son medios de guerra. El primero se utiliza para distribuir un código malicioso, mientras que el segundo se diseña para destruir información.[149]

2.3.2. Operaciones cibernéticas como método de guerra

Los métodos de guerra cibernéticos son las tácticas, técnicas y procedimientos cibernéticos con los que se conducen las hostilidades. En otras palabras, estos métodos se refieren a cómo se llevan a cabo las operaciones cibernéticas, que se distinguen de los instrumentos utilizados para conducirlas.[150]

Por ejemplo, una operación cibernética puede tener el objetivo de utilizar varias computadoras controladas por un programa maligno para sobrecargar la capacidad de manejar información que tiene un sistema en particular, es decir, una denegación de servicio distribuido. En este caso, el *botnet* califica como el

[149] *Ibidem*, pág. 250.
[150] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 103(b), págs. 452-453, párr. 4.

medio de guerra cibernético, mientras que la denegación de servicio distribuido es el método de guerra cibernético.[151]

En el ejemplo anterior la distinción es bastante clara. El *botnet* no causará por sí mismo una denegación de servicio distribuido, toda vez que sólo es el medio. Más bien, la denegación de servicio distribuido es causado por quien opera el *botnet*, es decir, la forma de emplear un medio. Asimismo, una denegación de servicio distribuido no es un medio, pues no se llevaría a cabo sin el *botnet*, por ende, la denegación de servicio distribuido es una forma de conducir las hostilidades, *id est*, un método de guerra cibernético.

Otro ejemplo es la utilización de medios cibernéticos para interferir con la capacidad del enemigo para comunicarse.[152] Una vez más, el instrumento que se emplee para lograr ese objetivo es el medio, y las interferencias con las comunicaciones, constituye en el método.

En ese sentido, en 2003 Estados Unidos se infiltró en el correo electrónico del Ministerio de Defensa de Irak para contactar con oficiales de ese gobierno y ordenarles que se rindieran de forma pacífica. Posteriormente, el ejército americano encontró equipamiento militar abandonado y arreglado de la misma forma en que se había instruido por correo.[153]

Las operaciones cibernéticas pueden ser conducidas como operaciones psicológicas dirigidas a la población civil, por ejemplo, a través de los medios de comunicación social. De igual forma, se podrían utilizar para engañar al enemigo,

---

[151] *Ibidem*, Regla 103(a), pág. 452, párr. 4.
[152] *Ibidem*, Regla 103(a), pág. 452, párr. 5.
[153] Cfr. HATHAWAY, Oona, *et al.*, "*The Law of Cyber-Attack*", *Op. Cit.*, pág. 839.

e.g. alterar los datos que el enemigo utiliza para rastrear la posición de sus aliados. En esa misma línea, se podría interferir la comunicación establecida por medio de drones.[154]

Un método de hacer la guerra puede ser el ataque a infraestructura civil o servicios esenciales para la población civil. Esto con la finalidad de afectar a la contraparte en general y que tenga que destinar recursos y atención a actividades diversas a la guerra en sí misma. Otra posibilidad es que esa infraestructura inicialmente civil se haya convertido en un objetivo militar. Cabe aclarar que se hace referencia a este método sin prejuzgar sobre su licitud.

Dichas disrupciones se llevan a cabo por medio del acceso a la red de información, luego al control del sistema y, finalmente, por la creación del efecto dañino al proceso industrial.[155]

Por ejemplo, el sector industrial es regularmente un objetivo de ataques cibernéticos cada año. En 2014, se reportó que este sector era objeto de aproximadamente 74 ataques por día a nivel global. Asimismo, en 2018, de todos los ataques a sistemas de control industrial, el 38.7% fueron dirigidos al sector energético.[156]

Los sucesos más notables se relacionan con Ucrania, que, en 2015 y 2016 sufrió ataques en este sector. El primer ataque resultó en la pérdida de electricidad por algunas horas para 230,000 personas habitantes de Ivano-

[154] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, págs. 34-35.
[155] *Ibidem*, pág. 23.
[156] *Ibidem*, pág. 62.

Frankivsk. Mientras que, en el segundo ataque, se afectó a un quinto de la población ucraniana en Kiev.[157]

En 2003, el virus *slammer*, con una capacidad de esparcimiento ultra rápida,[158] interfirió con la central nuclear Ohio Davis-Besse en Estados Unidos, desactivó las pantallas digitales, los sensores de radiación y temperatura durante casi 5 horas. Afortunadamente, un sistema análogo proveyó seguridad al funcionamiento de la central.[159]

Las instalaciones de tratamiento de agua también llegan a depender de sistemas de control industrial. En consecuencia, son vulnerables a sufrir un ataque cibernético que potencialmente concluiría en problemas de salud pública.[160]

En 1998, un niño de doce años entró sin permiso en el sistema de control de la presa Roosevelt de Arizona y tuvo a su disposición las compuertas que contenían 489 billones de galones de agua.[161]

En principio, cualquiera de estos ataques a una planta de energía o al sistema de suministro de agua sería un ataque prohibido en el contexto de un conflicto armado, toda vez que afectaría indistintamente a la población civil.

---

[157] *Idem*.

[158] Cfr. MOORE, David, *et al*, "The Spread of the Sapphire/Slammer Worm", en Center for Applied Internet Data Analysis, 2003, https://www.caida.org/catalog/papers/2003_sapphire/#:~:text=The%20Sapphire%20Worm%20was%20the,UTC%20on%20Saturday%2C%20January%2025.

[159] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 62.

[160] *Ibidem*, pág. 63.

[161] Cfr. HARRISON DINNISS, Heather, Cyber Warfare and the Laws of War, *Op. Cit.*, pág. 1.

2.4. El caso de la guerra en Ucrania

El 24 de febrero de 2022, Rusia invadió Ucrania a través de una serie de ataques convencionales que acompañó de una operación cibernética en contra de la red satelital *KA-SAT*, que era utilizada por el ejército ucraniano. El Instituto Europeo de Política Espacial realizó un breve reporte que informa sobre la operación cibernética en cuestión.[162]

Esta operación se desarrolló en dos fases. En primer lugar, se realizó una operación de denegación de servicio contra módems de *internet*, que estaban localizados en Ucrania y eran usados por el gobierno, la fuerzas armadas y servicios de seguridad.

En segundo lugar, quienes lanzaron la operación aprovecharon la configuración incorrecta de un dispositivo de red privada virtual para adentrarse en una red terrestre. A través de este dispositivo ganaron acceso remoto al segmento de gestión de la red *KA-SAT*. Esto, a su vez, permitió que se pudieran ejecutar comandos y facilitar la carga de un programa maligno llamado *acidrain*, el cual es del tipo limpiador, es decir, su función es dañar o destruir información en un sistema informático. Este programa se cargó en los módems de los usuarios y, posteriormente, borró el disco duro de los módems de *internet* de *KA-SAT*, por lo que se desconectaron de esta red y quedaron inutilizados.

Esta operación provocó un efecto en cadena en toda Europa que llegó no solamente instancias militares, sino que también perjudicó otros servicios que

[162] Cfr. INSTITUTO EUROPEO DE POLÍTICA ESPACIAL, “ESPI Short Report 1- The war in Ukraine from a space cybersecurity perspective”, Austria, octubre de 2022.

recurrían a *KA-SAT*. Alrededor de 9,000 suscriptores de *nordnet* —una compañía francesa de telecomunicaciones— sufrieron menoscabos. Aproximadamente 13,000 usuarios del servicio de *internet* proveído por *bigblu* fueron afectados en Alemania, Francia, Hungría, Grecia, Italia y Polonia. Adicionalmente, se impidió el acceso remoto de supervisión y control de 5,800 turbinas eólicas de la empresa energética alemana *enercon*.

Los efectos de esta operación provocaron que los proveedores de servicios ucranianos desviaran el tráfico de *internet* a Rusia. Esto implicó que los usuarios ucranianos se vieran obligados a navegar bajo las reglas rusas, lo que incluyó censura y control.

Este caso permite observar la actualidad de las operaciones cibernéticas empleadas en conflictos armados, así como la crucial importancia de saber cómo aplica el derecho internacional humanitario en estos casos.

2.5. Conclusiones

Con base en lo expuesto anteriormente, se puede concluir que:

- Cuando se hace mención del ciberespacio se hace referencia al tráfico de información entre dispositivos de distintos tipos que están interconectados en distintos niveles de alcance.
- Las operaciones cibernéticas se pueden explicar, en general, a través del modelo de cadena mortal y se distinguen dos tipos: de ataque a redes informáticas y de explotación de redes informáticas.

- La ciberguerra comprende operaciones lanzadas contra un ordenador o un sistema de ordenadores a través del ciberespacio, ya sea que dichas operaciones se constituyan en medios o métodos de guerra.
- Toda vez que las operaciones cibernéticas se pueden clasificar como medios o como métodos de guerra, están reguladas por el derecho internacional humanitario.
- La actualidad del uso de operaciones cibernéticas en la conducción de las hostilidades hace necesario abordar la aplicación del derecho internacional humanitario en tales casos.

Capítulo 3. El derecho internacional humanitario y la ciberguerra

En los capítulos anteriores se describió el funcionamiento del derecho internacional humanitario y el progreso en el contexto internacional respecto a las normas que aplican en el ciberespacio, así como el razonamiento técnico y legal que permite aplicar las normas del derecho internacional humanitario a los medios y métodos de guerra cibernéticos.

Ahora, se abordará cómo es que las normas del derecho de los conflictos armados regulan la ciberguerra. En particular, la Corte Internacional de Justicia adelantó en su opinión consultiva "*Legalidad de la amenaza o el uso de armas nucleares"* que:[163] a pesar de que el derecho convencional no cubra la regulación de ciertas armas, y aunque exista una diferencia cualitativa o cuantitativa entre las armas nuevas y las convencionales, los principios legales del derecho internacional humanitario gobiernan su utilización.

Asimismo, refirió que el carácter intrínsecamente humanitario de los principios jurídicos del derecho internacional humanitario "impregna todo el derecho de los conflictos armados y se aplica a todas las formas de guerra y a todos los tipos de armas, las del pasado, presente y futuro".[164]

En ese sentido, a continuación se abordan dos perspectivas sobre la regulación de la ciberguerra y los medios y métodos de guerra cibernéticos: 1) una evaluación jurídica de la legalidad de nuevos medios y métodos de guerra

[163] Cfr. CORTE INTERNACIONAL DE JUSTICIA, Legality of The Threat or Use of Nuclear Weapons, *Op. Cit.*, págs. 259-260, párr. 86.
[164] *Idem*: "…which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.".

cibernéticos a través del artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra”; y 2) una evaluación jurídica de la legalidad del empleo de medios y métodos de guerra cibernéticos al momento de emplearlos en operaciones cibernéticas únicamente o en conjunto con una operación militar tradicional, a través del contenido de los principios reguladores del derecho internacional humanitario.

En consecuencia, el propósito de este capítulo es demostrar que el derecho internacional humanitario actual, si bien no contiene normas específicas sobre el empleo de medios o métodos de guerra cibernéticos, sí provee de normas y principios reguladores lo suficientemente amplios y esenciales dentro del derecho internacional humanitario como para dotar de una regulación idónea a esta forma de conducir las hostilidades.

3.1. Artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra”

El artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra” dispone 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 Protocolo Adicional I a los Convenios de Ginebra o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante.”

El artículo 36 busca cambiar la temporalidad de la discusión sobre la legalidad del uso de armas nuevas, con el propósito de que el examen legal se realice de manera previa al uso del arma. En consecuencia, este artículo también derriba la justificación de que las armas nuevas no están cubiertas por reglas preexistentes del derecho internacional humanitario.[165] Las palabras "nuevo", "adquisición o adopción", indican que el requisito del artículo 36 es prospectivo, más que retroactivo.[166]

Esta provisión legal del "Protocolo Adicional I a los Convenios de Ginebra" no regula un arma en específico, sino que busca asegurar que las armas nuevas no contravengan el derecho internacional humanitario.[167] Aunque, incluso sin el artículo 36, cada Estado debe determinar si el empleo de un medio o método de guerra resultaría legal o no bajo las normas del derecho internacional humanitario.[168] El artículo 36 únicamente insta a los Estados a realizar el examen legal de las armas de manera previa a su utilización y resalta la importancia de hacer el examen desde la etapa más básica del desarrollo del arma nueva.

El artículo 36 pretende valorar la licitud del empleo de armas antes de que sean desarrolladas, adquiridas o incorporadas en el arsenal de un Estado. Al respecto, tras la valoración del arma en cuestión, pueden dimanar dos

---

[165] Cfr. KALSHOVEN, Frits, "*Reaffirmation and development of international humanitarian law applicable in armed conflicts: the conference of government experts (second session)*", en International Review of the Red Cross, Ginebra, junio-julio 1971, pág. 29.
[166] Cfr. McFARLAND, T. y ASSAAD, Z., "*Legal Reviews of in situ learning in autonomous weapons*", en Ethics and Information Technology, Vol. 25, Núm. 9, 2023, pág. 6.
[167] Cfr. JEVGLEVSKAJA, N., "*Legal Review of New Weapons: Origins of Article 36 of AP I*", en Finnish Yearbook of International Law, Finlandia, Vol. 25, 2017, pág. 111.
[168] *Idem*.

resultados:[169] 1) que el empleo del arma violaría el derecho internacional bajo cualquier circunstancia, o 2) que el empleo del arma violaría el derecho internacional solamente bajo algunas circunstancias y, por ende, se deben imponer restricciones a su utilización.

El artículo 36 del multicitado Protocolo tiene dos supuestos de aplicación: medios y métodos de guerra nuevos. Por ende, para aplicar el proceso de revisión conforme este artículo es necesario evaluar primero si se está frente a un medio o método de guerra que se considere nuevo.

Un medio o arma cibernética es cualquier dispositivo que esté diseñado, destinado o utilizado, con el fin de tener consecuencias violentas como causar la muerte o lesiones a personas o daños a objetos. Por ejemplo, un arma cibernética es una herramienta que permite llevar a cabo una operación por medios cibernéticos y que daña el funcionamiento de un sistema que controla la operación de una instalación de utilidad pública como una planta de tratamiento de agua.[170]

Los medios de hacer la guerra comprenden el equipamiento utilizado para controlar, facilitar o dirigir la conducción de las hostilidades. En ese sentido, no es necesario que las armas tengan efectos cinéticos para que se les considere como tales, por ejemplo, los gases o las armas biológicas.[171] Así, se deben considerar las armas cibernéticas de efectos cinéticos y no cinéticos.

---

[169] Cfr. LAWAND, K., Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos: medidas para aplicar el artículo 36 del Protocolo Adicional I de 1977, S.N.E., Comité Internacional de la Cruz Roja, Ginebra, 2006, pág. 4.
[170] Cfr. BOOTHBY, W., "*Methods and Means of Cyber Warfare*", en International Law Studies, U.S. Naval War College, Estados Unidos, Vol. 89, 2013, pág. 389.
[171] *Ibidem,* 388-389.

Las ciberarmas son las que pueden causar daño a las personas o a los objetos, por lo que, se excluyen las herramientas cibernéticas que están diseñadas únicamente para acceder a información.[172] Asimismo, un ciberataque es el que se lleva a cabo con ciberarmas que están diseñadas para resultar en daño físico tangible, o daño que causaría pérdida de funcionalidad y podría resultar en la necesidad de reemplazar los componentes físicos del sistema computacional.[173]

Por otro lado, los métodos cibernéticos son las tácticas, técnicas y procedimientos cibernéticos por medio de los cuales se conducen las hostilidades. Al respecto, la noción de hostilidades cubre más tipos de operaciones que aquellos que constituyen un ataque cibernético.[174]

Las operaciones más comunes son de reconocimiento, vigilancia y extracción de información.[175] Este tipo de operaciones no son susceptibles de ser reguladas por los principios reguladores del derecho internacional humanitario, toda vez que no tienen un efecto que pudiera resultar prohibido o delimitado.

El reconocimiento de cualquier grado no resultará en perjuicio para civiles o militares. Consecuentemente, no se requiere medir proporcionalidad o necesidad militar alguna, pues no habrá daño incidental o sufrimiento innecesario. En todo caso, la pregunta es ¿qué pasará con la información que se

[172] Cfr. BOULANIN, Vincent y VERBRUGGEN, Maaike, Article 36 reviews: dealing with the challenges posed by emerging technologies, S.N.E., SIPRI, Suecia, 2017, pág. 9.
[173] *Ibidem*, págs. 9-10.
[174] *Ibidem*, pág. 10.
[175] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 12.

obtenga a partir de las actividades de reconocimiento, vigilancia o extracción de datos? ¿Se utilizarán para emplear algún medio o método de guerra ilícito?

En realidad, lo que se haga con esa información no vuelve ilícita su recolección, pues son dos momentos diferenciados. Al respecto, son precisas las siguientes consideraciones: primero, ninguna de las operaciones referidas está prohibida en sí misma, como los medios de guerra que sí lo están por su naturaleza, sin importar cómo se usen; segundo, si la información recabada se utilizara para emplear un medio o método de guerra contrario a derecho, sería el propio medio o método el que estaría prohibido, no la información, pues constituyen actividades separadas.

Ahora bien, en el ciberespacio es pertinente considerar todos los dispositivos, materiales, instrumentos, mecanismos, equipamientos o programas diseñados para o usados en un ataque. Esto incluye cualquier tipo de *botnet*, programa maligno o programa espía usado para ganar acceso a una computadora para preparar o apoyar en un ataque.[176]

Las armas que deben ser sometidas a este examen jurídico son las de todo tipo. Esto abarca las armas que están en desarrollo o que ya existen, pero que recientemente van a ser adquiridas, o bien, las armas que ya existían, pero serán modificadas.[177]

[176] Cfr. BOULANIN, Vincent y VERBRUGGEN, Maaike, Article 36 reviews: dealing with the challenges posed by emerging technologies, *Op. Cit.*, pág. 10.
[177] Cfr. LAWAND, K., Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos: medidas para aplicar el artículo 36 del Protocolo Adicional I de 1977, *Op. Cit.*, págs. 8-9.

La determinación bajo el artículo 36 del "Protocolo Adicional I a los Convenios de Ginebra" se debe hacer sobre la base del uso normal del arma, al menos como se anticipa su uso normal al momento de la evaluación.[178] Esto, debido a que, en general, la mayoría de las armas podrían utilizarse de forma contraria al derecho internacional humanitario.[179] En consecuencia, el examen se limita razonablemente sólo al uso normalmente previsto.

Cuando una ciber arma está a disposición de actores distintos a los que la desarrollan, ya sea porque la robaron o porque se filtró, estos otros actores pueden utilizar ingeniería inversa y resignificar su propósito para fines maliciosos.[180] Esta posible utilización del arma no se consideraría en el examen jurídico del arma en cuestión, pues no está prevista dentro del uso normal del medio cibernético.

Un arma se considera nueva en dos situaciones: 1) si es nueva para el Estado que planea adquirirla, aunque el arma ya existiera con anterioridad; y, 2) si es de creación reciente y su adquisición coincide con el primer uso del arma.[181]

Asimismo, un arma modificada de tal forma que su comportamiento sea alterado y resulte legalmente significante, debe ser considerada como nueva en términos del artículo 36 del multirreferido Protocolo. Consecuentemente, se debe

---

[178] Cfr. SANDOZ, Yves, *et al.* (eds.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, *Op. Cit.*, párr. 1466 y 1480.
[179] Cfr. McCLELLAND, J., "*The Review of weapons in accordance with Article 36 of Additional Protocol I*", en International Review of the Red Cross, Ginebra, Vol. 85, Núm. 850, 2003, págs. 407-408.
[180] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Ginebra, 2019, pág. 27.
[181] Cfr. McCLELLAND, J., "*The Review of weapons in accordance with Article 36 of Additional Protocol I*", *Op. Cit.*, pág. 404.

realizar un examen legal sobre su compatibilidad con el derecho internacional humanitario, incluso si antes de la modificación había sido sometida al mismo examen.[182]

No todas las modificaciones a un arma conllevan a la necesidad de realizar una revisión legal bajo los términos del artículo 36, pues no todas las modificaciones implican un cambio sustancial en las capacidades del arma.[183] Por ende, el impacto de las modificaciones se debe valorar caso por caso.

Con respecto a las normas bajo las cuáles se debe analizar el medio o método, el Protocolo Adicional refiere que el análisis legal de la licitud debe revisarse a la luz del "Protocolo Adicional I a los Convenios de Ginebra" o de cualquier otra norma de derecho internacional aplicable al Estado en cuestión. Esto último abre las puertas a las distintas fuentes de derecho internacional.[184] En consecuencia, la forma más adecuada de proceder es comenzar por valorar las normas convencionales después las consuetudinarias y finalmente los principios generales de derecho.

Asimismo, una aproximación estructurada a la licitud de nuevos medios o métodos de guerra conlleva comenzar por valorar si éstos ya se encuentran explícitamente prohibidos o restringidos, ya sea por el derecho convencional

[182] Cfr. McFARLAND, T. y ASSAAD, Z., "*Legal Reviews of* in situ *learning in autonomous weapons*", *Op. Cit.*, pág. 5.
[183] Cfr. McCLELLAND, J., "*The Review of weapons in accordance with Article 36 of Additional Protocol I*", *Op. Cit.*, pág. 404.
[184] Cfr. LAWAND, K., Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos: medidas para aplicar el artículo 36 del Protocolo Adicional I de 1977, *Op. Cit.*, pág. 9.

positivo o por una norma dimanante de otra fuente. De no ser el caso, entonces corresponde evaluar las prohibiciones o restricciones generales.[185]

Cuando se evalúa el medio o método de guerra conforme a las prohibiciones o restricciones generales, debe tomarse en consideración la posible aplicación en la práctica. Para esto, se contemplan las características, el uso previsto y los efectos previsibles.[186]

Por ejemplo, en el caso de los *botnets*, puede tomarse en consideración que aquellos que operan mediante el método de comunicación por pares suelen reproducirse de forma automática, por lo que no discriminan entre los posibles objetivos. En consecuencia, hay una posibilidad de que no sea compatible con el "Principio de Distinción".

Así, para realizar una evaluación adecuada, debe considerarse: 1) la descripción técnica del arma; 2) el funcionamiento técnico del arma; 3) las consideraciones relativas a la salud; y, 4) las consideraciones relativas al medio ambiente.[187]

La descripción técnica contempla las características del arma, el empleo para el que se concibió y los medios que utiliza para causar efectos. El funcionamiento técnico implica la precisión y la fiabilidad del mecanismo de ataque, el área que cubre el arma, el alcance de sus efectos y la posibilidad de controlarlos temporal y espacialmente.

---

[185] *Ibidem*, pág. 14.
[186] *Idem*.
[187] *Ibidem*, págs. 17-19.

Sobre los efectos en la salud de las personas, deben tomarse en cuenta las pruebas científicas existentes sobre los posibles efectos del arma, cómo se prevé que impactará en las víctimas, cuál es el índice de mortalidad previsto, si pudiera causar alteraciones a largo plazo o permanentes, así como la posibilidad de lidiar médicamente con los efectos.

En cuanto al medio ambiente, deben sopesarse los estudios científicos sobre los efectos del arma en el medio ambiente natural, qué daño se prevé causar, cuánto durará, si será posible revertirlo y si tendrá efectos en la población civil, ya sea directa o indirectamente.

Todas estas reflexiones se deben atender en el examen que se realice sobre la licitud del arma en sus distintas etapas: estudio, desarrollo, adquisición o adopción del arma. El estudio incluye la investigación y diseño del arma; el desarrollo contempla el avance en la creación del arma y la prueba de prototipos; mientras que, la adquisición abarca la compra de armas en existencia. En caso de la adopción de una modificación técnica, también debe examinarse su licitud en cuanto sea posible.[188]

Cobra relevancia tener en cuenta lo siguiente: 1) examinar el arma en las distintas fases de su creación, 2) considerar el estado actual y posible desarrollo del derecho internacional humanitario, 3) disponibilidad de toda la información sobre las características del arma, y 4) actualizar la revisión del arma conforme aumenta la información disponible sobre su funcionamiento.[189] Esto es debido a

[188] *Ibidem*, págs. 22-23.
[189] Cfr. McCLELLAND, J., "*The Review of weapons in accordance with Article 36 of Additional Protocol I*", *Op. Cit.*, pág. 413..

que, la revisión legal del arma en cuestión resulta efectiva si se tiene en cuenta la mayor cantidad de información disponible.

Otras consideraciones específicamente relevantes en relación con armas cibernéticas son: 1) el riesgo de que afecten o dañen sistemas civiles y redes civiles debido a la conexión de redes civiles y militares, y 2) el riesgo de que puedan replicarse a sí mismas de forma indiscriminada.[190]

Los ataques cibernéticos suelen operar de manera ubicua.[191] En general, esto implica que un arma cibernética puede fácilmente tener efectos en redes civiles, lo que la volvería de efectos indiscriminados inherentemente.[192]

Los efectos de las operaciones cibernéticas deben tenerse en cuenta al momento de realizar el examen legal, particularmente:[193] 1) los efectos directos sobre el sistema objetivo y el impacto sobre la instalación en la cual opera el sistema, así como 2) el impacto sobre las personas directamente afectadas por la pérdida de utilidad y funcionalidad del sistema en cuestión.

Al respecto, en la doctrina se ha referido que el uso de ciber infraestructura perteneciente a Estados neutrales en un conflicto armado es una violación al derecho internacional humanitario.[194] Sin embargo, esto es debatible. Cabe mencionar que, si esto fuera así, entonces las posibilidades de llevar a cabo operaciones cibernéticas lícitas, sin utilizar la infraestructura cibernética de otros

---

[190] Cfr. BOULANIN, Vincent y VERBRUGGEN, Maaike, Article 36 reviews: dealing with the challenges posed by emerging technologies, *Op. Cit.*, pág. 12.
[191] Cfr. TALBOT, Eric, "*Cyber Warfare and Precautions against the Effects of Attacks*", en Texas Law Review, Vol. 88, 2009, pág. 1542.
[192] Cfr. BOULANIN, Vincent y VERBRUGGEN, Maaike, Article 36 reviews: dealing with the challenges posed by emerging technologies, *Op. Cit.*, pág. 10.
[193] *Ibidem*, pág. 12.
[194] *Ibidem*, pág. 13.

Estados, se verían reducidas dramáticamente, así como las opciones de medios cibernéticos a emplear en cada operación.

Realizar operaciones cibernéticas desde ubicaciones remotas, y aprovechar la gran interconectividad existente, es la gran ventaja que ofrece el ciberespacio. Sin el aprovechamiento de esta virtud, las operaciones cibernéticas se limitarían a operaciones de corto alcance y de manera prácticamente directa.

Si se considera que el *internet* es, en general, una infraestructura cibernética de índole dual porque puede emplearse para propósitos civiles y militares, entonces el punto al realizar una operación cibernética no es evadir el uso del *internet*, sino emplearlo de tal forma que los ataques cibernéticos delimiten el impacto final únicamente al objetivo militar.

A fin de cuentas, lo civil se transita para llegar a lo militar en el caso de operaciones cibernéticas y esto no contraviene el derecho internacional humanitario.[195] Los códigos militares viajan en el ciberespacio y se dividen en distintos paquetes informáticos que pueden viajar en diversos canales civiles y atravesar varios sistemas civiles. En un ataque cibernético, un rango amplio de infraestructuras cibernéticas físicas —servidores, *routers*, cables o satélites— pueden ser utilizadas para hacer una contribución efectiva a las actividades militares.[196]

---

[195] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 151, pág. 556.

[196] Cfr. GEISS, R. y LAHMANN, H., "*Cyber warfare: applying the principle of distinction in an interconnected space*", en Israel Law Review, Cambridge University Press, Reino Unido, Vol. 45, Núm. 3, 2012, pág. 386; KELSEY, Jeffrey, "*Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*", en Michigan Law Review, The Michigan Law Review Association, Estados Unidos, 2008, Vol. 106, Núm. 7, pág. 1433.

No se debe pensar en prohibir el tránsito por infraestructura civil, esto podría redundar en el incumplimiento de una norma tan restrictiva que resulte absurdamente difícil de cumplir. Al mismo tiempo, el hecho de que la infraestructura civil sea utilizada ocasionalmente para propósitos militares no significa que deba ser atacada en su totalidad o en cualquier momento, pues esto podría resultar en una falta de cumplimiento con la obligación de tomar las debidas precauciones y procurar la proporcionalidad en los ataques.

Por otro lado, se debe tomar en cuenta que las herramientas cibernéticas pueden permitir controlar los sistemas computacionales del adversario en un conflicto armado. Esto es relevante en tanto que, la parte beligerante que tome control de un sistema así, no debe utilizarlo de forma contraria al derecho internacional humanitario, por ejemplo, para emplear algún arma prohibida en posesión de la parte cuyo sistema es atacado.[197]

Otro aspecto relevante es si la operación cibernética afectaría la funcionalidad de un sistema o dañaría los datos del sistema sin causar daño físico, a la vez que identificar los alcances de los efectos de la operación, directos e indirectos.[198]

Algunas recomendaciones de restricciones a armas cibernéticas son:[199]

- Restricciones sobre las condiciones de uso, como definir estrictamente el objetivo y la red a través de la que se utilizará el arma cibernética;

[197] Cfr. BOULANIN, Vincent y VERBRUGGEN, Maaike, Article 36 reviews: dealing with the challenges posed by emerging technologies, *Op. Cit.*, pág. 13.
[198] *Idem*.
[199] *Ibidem*, pág. 14.

- No emplear programas malignos que puedan replicarse a sí mismos, además de incluir un comando de destrucción automática una vez que el objetivo de la operación sea alcanzado; y,
- Realizar un mapeo de red antes de iniciar una operación cibernética, en función de precisar los alcances de sus efectos.

Actualmente, la evaluación de armas cibernéticas puede verse ampliamente beneficiada del uso de c*yber ranges*, que son ambientes cibernéticos simulados en los que se puede evaluar la interacción entre atacantes y defensores.[200]

La determinación que realice cualquier Estado sobre la legalidad del uso de cierta arma no es vinculante internacionalmente, ya sea que la considere prohibida o permitida.[201] Asimismo, los Estados no están obligados a expresar públicamente el resultado de la evaluación.[202] Aun así, el Estado que realice la evaluación debe tener presente el resultado de ésta.

El artículo 36 del "Protocolo Adicional I a los Convenios de Ginebra" puede tener una solución a los retos y complejidades de los ataques cibernéticos.[203] Lamentablemente, todavía en tiempos recientes, el número de Estados que llevan a cabo un examen legal completo de armas es insignificante: alrededor de

---

[200] BRANGETTO, Pascal, ÇALIŞKAN, Emin y RÕIGAS, Henry, Cyber Red Teaming: Organisational, technical and legal implications in a military context, S.N.E., CCDCOE, Tallin, 2015, pág. 29.
[201] Cfr. SANDOZ, Yves, *et al.* (eds.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, S *Op. Cit.*, párrs. 1469 y 1481.
[202] *Ibidem*, párrs. 1470 y 1481.
[203] Cfr. ROSANA, C., "*A Game of Code: Challenges of Cyberspace as a Domain of Warfare*", en Strathmore Law Review, Vol. 3, 2018, pág. 70.

30.[204] Aunque, este artículo impone la obligación de establecer procedimientos internos con miras a lidiar con el problema de la ilegalidad. Por ende, las demás partes contratantes pueden pedir información al respecto.[205]

Finalmente, resulta evidente que la evaluación que exige el artículo 36 del multicitado Protocolo cubre de manera amplia y exhaustiva las características de los nuevos medios y métodos de guerra cibernética, así como su empleo práctico. Por consiguiente, es una disposición legal apropiada para abordar el desarrollo constante y vertiginoso de la manera de hacer la guerra; todo de conformidad con el contenido esencial del derecho internacional humanitario.

3.2. Principios reguladores del derecho internacional humanitario

A continuación, se analizará la aplicación de los principios consuetudinarios que rigen el derecho internacional humanitario en los medios y métodos de guerra cibernética, es decir, los principios de distinción, proporcionalidad, necesidad militar y humanidad.

3.2.1. Distinción

[204] Cfr. JEVGLEVSKAJA, N., "*Legal Review of New Weapons: Origins of Article 36 of AP I*", *Op. Cit.*, pág. 40.
[205] Cfr. SANDOZ, Yves, *et al.* (eds.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, *Op. Cit.*, párr. 1482.

El ciberespacio es probablemente una infraestructura construida y poseída por civiles en un 90%.[206] Consecuentemente, cabe cuestionar en qué medida es lícito el uso del ciberespacio para realizar operaciones con fines beligerantes, toda vez que el derecho internacional humanitario exige la protección de las personas y bienes civiles.

La conducción de las hostilidades de forma tradicional ocupa métodos cada vez más sofisticados para estimar el posible daño colateral de una operación militar; empero, tal metodología carece del mismo desarrollo en operaciones cibernéticas.[207]

Al estimar la predominancia del carácter civil de la infraestructura cibernética, parecería que el uso de operaciones cibernéticas como medio o método de guerra queda ampliamente restringido.

A continuación, se aborda la relevancia de este hecho de frente al "Principio de Distinción".

El "Principio de Distinción" implica que las partes en un conflicto deben diferenciar en todo momento entre población civil y combatientes, así como entre bienes de carácter civil y objetivos militares. En consecuencia, las operaciones cibernéticas que califican como ataque deben dirigirse únicamente contra objetivos militares —artículo 48 del "Protocolo Adicional I a los Convenios de Ginebra"—.[208]

---

[206] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 30.
[207] *Ibidem*, pág. 16.
[208] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 1, pág. 3; Cfr. SCHMITT, Michael N., Tallinn

Los objetivos militares son aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyen eficazmente a la acción militar y cuya destrucción total o parcial, captura o neutralización ofrece, en las circunstancias del caso, una ventaja militar definida —artículo 52(2) del "Protocolo Adicional I a los Convenios de Ginebra"—.[209]

La infraestructura cibernética puede calificar como objetivo militar.[210] Esta infraestructura cubre dispositivos de comunicación, de almacenamiento e informáticos sobre los que se construyen y funcionan los sistemas de información.[211] Esto siempre que cubran los requisitos exigidos por el derecho internacional humanitario para ser objetivos militares.

Los objetivos militares pueden calificar como tales bajo cuatro criterios: naturaleza, ubicación, propósito o uso. La naturaleza se refiere al carácter inherente de un objeto que es fundamentalmente militar y que está diseñado para contribuir a las actividades militares. Por ejemplo, sistemas militares de comando, control, comunicaciones, informática, inteligencia, vigilancia y reconocimiento. Estos son objetivos militares independientemente de quién los opere.[212]

Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Reglas 94 y 99, págs. 422 y 434.

[209] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 8, pág. 29.

[210] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 100, págs. 435-436.

[211] *Ibidem*, Glosario, pág. 564.

[212] *Ibidem*, Regla 100, pág. 438.

Sobre el criterio de ubicación, este se refiere a un área que tiene importancia militar particular. Una dirección IP no es una ubicación, aunque se asocie con la infraestructura cibernética que sí puede calificar como un objetivo militar.[213]

El criterio de uso implica que un objeto o instalación civil utilizada para finalidades militares se torna en un objetivo militar. Por ejemplo, el uso de una red informática civil para propósitos militares.[214] El uso militar de una computadora contempla desde la planificación de atentados hasta simples tareas administrativas, es decir, cubre el trato o almacenamiento de datos militares y cifrado o descifrado de códigos.[215] Prácticamente contempla todo lo que contribuye a los propósitos militares desde el nivel mínimo.

En contraste, el criterio de propósito se refiere al uso futuro que se pretende dar a un objeto, *v.gr.* si hay información confiable que revele que una parte beligerante está a punto de comprar *hardware* —elementos físicos— o *software* —soporte lógico— informático para propósitos militares, esos artículos se convierten en objetivos militares.[216]

Un objetivo militar califica como tal a través de al menos uno de estos criterios si el objeto en cuestión hace una contribución efectiva a las actividades militares, *id est*, contribuye a la ejecución de las operaciones beligerantes o apoya directamente las actividades militares del enemigo.[217]

---

[213] *Idem*.
[214] *Ibidem*, págs. 439-440.
[215] Cfr. DINSTEIN, Yoram, "*The Principle of Distinction and Cyber War in International Armed Conflicts*", *Op. Cit.*, pág. 263.
[216] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 100, págs. 439-440.
[217] *Idem*.

Por ejemplo, un sitio *web* que transmite mensajes cifrados a las fuerzas armadas de la contraparte genera una contribución eficaz a la acción militar, por lo que la infraestructura cibernética que soporta el sitio *web* es un objetivo militar. Esto no implica que la red informática en su totalidad necesariamente califica como objetivo militar.[218] Es decir, incluso después de identificar un objeto como objetivo militar se deben tomar las precauciones necesarias para realizar un ataque proporcional.

Para saber si el ataque a dichos objetivos militares ofrece una ventaja militar definida se debe valorar el ataque como un todo y no únicamente cada acción del ataque en particular, lo que no implica analizar todo el contexto de la guerra en cada operación. Por ejemplo, realizar un ataque cibernético contra un objetivo militar alejado del lugar donde se planea realizar una operación importante. La operación cibernética se constituye en una artimaña meramente para engañar al enemigo en cuanto a la ubicación real de la operación central. El éxito del engaño puede determinar el éxito de la operación en conjunto.[219]

Así, si la infraestructura civil o cualquier otro objeto civil no es un objetivo militar, no debe ser atacado. Por ejemplo, plantas de agua o electricidad, propiedad privada o equipo e infraestructura gubernamental dedicada a tecnologías de la información y comunicación de carácter civil. Esto es independiente de si la infraestructura civil es calificada como crítica o no.[220]

---

[218] *Idem*.

[219] *Ibidem*, Regla 100, pág. 442.

[220] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, “Cyber operations during armed conflict: the principle of distinction”, en Comité Internacional de la Cruz Roja, Ginebra, Suiza, 7 de marzo de 2023, pág. 1, [en línea] https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf.

Esto no significa que la infraestructura de tecnologías de la información y comunicación civil no pueda ser utilizada de paso para dirigir una operación militar. El “Principio de Distinción” únicamente limita a no dirigir ataques contra personas u objetos civiles.

Un caso de violación al “Principio de Distinción” sucedería si se realizara una operación cibernética que impidiera el acceso a *internet* de forma generalizada. Aunque esta operación pudiera tener el propósito original de afectar a la contraparte en un conflicto armado.

Por ejemplo, una parte beligerante podría pretender evitar el acceso a *internet* en una región determinada con el propósito de afectar la comunicación entre los miembros de las fuerzas armadas de la contraparte. Si se realizara esta operación y se privara de *internet* a la población de forma generalizada, se violaría el "Principio de Distinción”.

Por otro lado, una operación cibernética que se vale del *internet* que la población en una región utiliza de forma general únicamente para enviar un programa maligno a un objetivo militar, no sería contrario a derecho internacional humanitario.

Esto se clarifica si atendemos a un ejemplo de la conducción de hostilidades tradicional: transitar por territorio mayormente habitado por población civil para llegar al objetivo militar no es violatorio del derecho internacional humanitario. Lo que podría contravenir el derecho internacional humanitario sería atacar ese territorio habitado por la población civil.

En el ambiente de las tecnologías de la información y la comunicación, la población civil y los miembros de las fuerzas armadas usualmente utilizan la

misma infraestructura de *internet* —cables, satélites, *routers* y nodos—, así como también pueden coincidir en medios de comunicación digital, almacenamiento y otro tipo de servicios.[221]

Este tipo de objetos, que son utilizados tanto para propósitos civiles como militares, son conocidos como objetos de uso dual y únicamente pueden ser atacados si cumplen con los requisitos para ser objetivos militares. En cuyo caso, todavía es ineludible la obligatoriedad de los principios del derecho internacional humanitario.[222]

Por ejemplo, si los servicios civiles de correo electrónico se utilizan para transmitir información militarmente útil, la infraestructura utilizada para transmitirla puede considerarse un objetivo militar.[223] Es preciso notar que, básicamente no hay distinción entre computadoras civiles y militares, cualquiera podría ser parte de una operación militar y ser utilizada al mismo tiempo para propósitos civiles.[224] Por ende, es relevante realizar una evaluación constante para verificar la licitud de atacar objetivos militares.

Las obras e instalaciones que contienen fuerzas peligrosas, como presas, diques y centrales nucleares de energía eléctrica, aunque pueden llegar a ser objetos de uso dual, se les debe una protección especial:[225] las partes

---

[221] *Idem*.
[222] *Ibidem*, pág. 2.
[223] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 100, pág. 444.
[224] Cfr. GEISS, R. y LAHMANN, H., "*Cyber warfare: applying the principle of distinction in an interconnected space*", *Op. Cit.*, pág. 389.
[225] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 42, pág. 139; Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 140, pág. 529.

beligerantes deben tener un cuidado particular con este tipo de instalaciones para evitar la liberación de las fuerzas peligrosas y la consecuente pérdida importante en la población civil —artículo 56(1) del "Protocolo Adicional I a los Convenios de Ginebra"—.

Una expresión del "Principio de Distinción" es que está prohibido realizar ataques indiscriminados. Los ataques de este carácter son aquellos que:[226] a) no se dirigen contra un objetivo militar específico, b) los que emplean un medio o método de guerra que no puede ser dirigido contra un objetivo militar específico, o c) aquellos que emplean un medio o método de guerra cuyos efectos no pueden ser limitados como requiere el derecho internacional humanitario —artículo 51(4) del "Protocolo Adicional I a los Convenios de Ginebra"—.

Al respecto, estos 3 supuestos se actualizarían en los siguientes ejemplos:[227] a) una operación cibernética que pretende borrar la información de las computadoras de todas las agencias gubernamentales del adversario, sin distinguir agencias civiles y militares; b) liberar un programa maligno en una red abierta y que tenga la capacidad de explotar vulnerabilidades en sistemas civiles y militares, así como propagarse a sí mismo; y, c) llevar a cabo una operación cibernética dirigida contra un objetivo militar que, una vez comenzada, no puede ser limitada y esparce sus efectos sin control, así como causa daño desproporcionado a objetivos no militares.

---

[226] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Reglas 11 y 12, págs. 37 y 40.
[227] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, "*Cyber operations during armed conflict: the principle of distinction*", *Op. Cit.,* pág. 2.

Este tipo de operaciones se constituirían en ataques cibernéticos que deben ser regulados bajo los principios del derecho internacional humanitario, toda vez que, como se explicó en el capítulo anterior, un ataque cibernético es el que utiliza medios cibernéticos con el propósito de causar un perjuicio a una computadora, a un sistema de computadoras o a la información que contienen. Estas son las llamadas operaciones de ataque a redes informáticas, que cubren operaciones de engaño, interrupción, negación, degradación y destrucción.

En contraste, operaciones que no califican como ataque son: el hackeo de una computadora para reunir inteligencia o plantar un gusano informático.[228]

Las operaciones cibernéticas deben realizarse de conformidad con el "Principio de Distinción". Para esto, es preciso que los medios o métodos que se pretende utilizar se empleen con la precisión suficiente para dirigirse hacia un objetivo específico.[229]

En la realización de las operaciones cibernéticas, se deben tomar todas las precauciones factibles para evitar o minimizar daño a la población y objetos civiles mediante:[230] 1) la verificación de que los objetivos son militares, 2) la elección adecuada de medios y métodos de guerra, y 3) la valoración de los posibles efectos del ataque —artículo 57(2)(a)(i)-(iii) del "Protocolo Adicional I a los Convenios de Ginebra"—.

---

[228] Cfr. DINSTEIN, Yoram, "*The Principle of Distinction and Cyber War in International Armed Conflicts*", *Op. Cit.*, pág. 264.
[229] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, "*Cyber operations during armed conflict: the principle of distinction*, *Op. Cit*., pág. 2.
[230] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Reglas 15, 16, 17, 18, págs. 51, 55, 56, 58

Si bien es posible que todo el *internet* pueda ser, al menos potencialmente, usado para propósitos militares, la realidad es que no es utilizado de esa manera en su totalidad. Así que, aunque puede ser un bien de uso dual, incluso ocasional, siempre debe distinguirse cuando ciertamente se usa para fines militares y cuando no.

Si un atacante no puede reunir información confiable sobre la naturaleza de un sistema propuesto como objetivo militar, se debe limitar el alcance del ataque solamente a aquellos componentes o capacidades del sistema sobre los que exista información suficiente para verificar su condición de objetivos lícitos.[231]

Igualmente, la información disponible debe utilizarse para determinar qué medio o método cibernético es más apropiado para desarrollar una operación militar. Por ejemplo, para insertar un programa maligno en una red militar cerrada. En este caso, un método para hacerlo sería utilizar una unidad USB.[232]

En particular, los gusanos suelen ser difíciles de contener una vez que se liberan, toda vez que se replican y esparcen de forma rápida y eficiente. Por ejemplo, el gusano *conficker* fue liberado en 2008 y en 2018 aún infectaba sistemas.[233] La utilización de este tipo de programas malignos requiere restricciones que lo hagan compatible con el derecho internacional humanitario, como delimitar con mayor certeza los objetivos, o bien, no emplearlos.

---

[231] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 115, pág. 479.
[232] *Ibidem*, Regla 116, pág. 480.
[233] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 56.

Consecuentemente, se debe valorar el posible impacto de las operaciones cibernéticas, probar los medios cibernéticos en ambientes de tecnologías de la información y la comunicación similares a los objetivos, así como se deben emplear las medidas que permitan prevenir o detener los posibles efectos indiscriminados que pueda generar el uso de un medio o método de guerra cibernético.[234]

Algunos expertos han enfatizado que la falta de certeza sobre los efectos de una operación es una característica inherente de las operaciones cibernéticas. Como ejemplo, refieren que las herramientas cibernéticas consisten eminentemente en *software*, por lo que siempre existe el riesgo de tener errores en el código de programación que podrían llevar a efectos imprevistos y no intencionales.[235] Empero, esto no es así. Tanto puede haber operaciones cibernéticas con un alto nivel de precisión como operaciones con poca certeza en la delimitación de sus objetivos.

Existe una obligación de hacer todo lo fácticamente posible por separar a la población y objetos civiles de los objetivos militares —artículo 58 del "Protocolo Adicional I a los Convenios de Ginebra"—.[236] Una forma de mitigar el peligro que corren los sistemas civiles de sufrir ataques o daños colaterales es:[237] remover

[234] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, "*Cyber operations during armed conflict: the principle of distinction*", *Op. Cit.*, pág. 2.
[235] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 38.
[236] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Reglas 22-24, págs. 68, 71 y 74; Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 121, pág. 487.
[237] Cfr. GEISS, R. y LAHMANN, H., "*Cyber warfare: applying the principle of distinction in an interconnected space*", *Op. Cit.*, pág. 392.

físicamente y desconectar las redes civiles de otras redes y de la infraestructura cibernética general; especialmente las redes civiles altamente sensibles y soportes primarios de la infraestructura, cuya funcionalidad es esencial para la población civil.

Sin embargo, esto requeriría una remodelación estructural de la forma en la que actualmente está construida la infraestructura del ciberespacio. Algo que podría no ser factible para las partes beligerantes.[238]

Cabe tener en consideración que, las herramientas cibernéticas pueden diseñarse para afectar un sistema o programa en particular, como aquellos programas utilizados para afectar la vulnerabilidad del sistema operativo *linux* o *windows*. Otros ejemplos son los programas *stuxnet*, *vpnfilter* y *triton*.[239] En el caso del primero, se programó para operar en el sistema de una instalación específica; el segundo operaba en sistemas de nodos con una vulnerabilidad particular; el tercero tenía por objetivo vulnerabilidades en los sistemas de seguridad instrumentados t*riton*.

Por otro lado, en las operaciones de denegación de servicio distribuido los actores pueden obtener información incompleta sobre el nivel de red y las interconexiones, por lo que, es probable que las consecuencias no siempre puedan ser valoradas con precisión antes de realizar el ataque. Además, si hablamos de *software* malicioso que está programado para esparcirse automáticamente, entonces claramente se puede advertir que sus efectos son

[238] *Ibidem*, pág. 393.
[239] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 55.

inciertos.[240] Por ende, el uso de una operación de denegación de servicio distribuido tiene posibilidades limitadas de respetar el derecho internacional humanitario.

Como resultado, es pertinente valorar cada medio y método de guerra para saber si su empleo puede cumplir o no con el "Principio de Distinción", ya sea en todas o en algunas circunstancias.

3.2.2. Proporcionalidad

El "Principio de Proporcionalidad" implica que un ataque cibernético está prohibido cuando:[241] sea de prever que causará incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista —artículo 51(5)(b) del "Protocolo Adicional I a los Convenios de Ginebra"—.

En ese entendido, este principio indica que el daño civil incidental puede ser lícito bajo los parámetros que fija. Para saber si un ataque que causa daño colateral es lícito, se debe evaluar la relación entre el daño incidental que el atacante espera razonablemente que sea producido y la ventaja militar que el atacante anticipa que ganará como resultado del ataque. Cabe resaltar que, un

[240] *Ibidem*, págs. 30 y 38.

[241] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 113, pág. 470; Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 14, pág. 46.

ataque cibernético puede causar daño colateral tanto durante el tránsito por la infraestructura cibernética como en el ataque mismo.[242]

Por ejemplo, el Sistema de Posicionamiento Global es un objeto de uso dual que podría ser un objetivo militar, empero, un ataque a éste podría implicar daños desproporcionados al evitar que la población civil tenga acceso a información esencial como información de navegación utilizada por barcos mercantes o aviones civiles.[243]

Este principio prevé tres situaciones: la muerte incidental de población civil, daño a la población civil y daño a objetos civiles. Una operación cibernética no siempre generará ese tipo de efectos, toda vez que puede desactivar una red informática sin causar daño.[244] Aunque el daño previsto por esta norma incluye la pérdida de funcionalidad,[245] por lo que también las operaciones cibernéticas que vuelven inservible un dispositivo están contempladas bajo esta disposición.

La evaluación del posible daño civil incidental incluye daño directo e indirecto, como resultado de operaciones cibernéticas. El daño directo contempla los efectos causados en el objetivo específico; mientras que, el daño indirecto cubre las demás consecuencias que derivan del ataque en cuestión.[246] Por ejemplo, la muerte de pacientes en unidades de tratamiento intensivo causada

---

[242] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 113, pág. 471.
[243] *Idem*.
[244] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, "Cyber operations during armed conflict: the principle of proportionality", en Comité Internacional de la Cruz Roja, Ginebra, Suiza, 7 de marzo de 2023, pág. 2, [en línea] https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/04_proportionality-0.pdf.
[245] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 113, pág. 472.
[246] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, "*Cyber operations during armed conflict: the principle of proportionality*", *Op. Cit.*, pág. 2.

por una operación cibernética sobre la red eléctrica que resulta en el corte de suministro de energía.[247]

El estándar para saber si un ataque cibernético podría causar daño civil incidental requiere que la situación se valore desde la perspectiva de un comandante razonable, es decir, alguien con entrenamiento y experiencia en el arte militar, quien, de buena fe, utiliza toda la información y recursos razonablemente disponibles en cada circunstancia. En el caso de ciberataques, esto podría incluir el asesoramiento de un experto técnico.[248]

El "Principio de Proporcionalidad" no exige que el daño y la ventaja esperada sean determinadas con certeza absoluta.[249] Sin embargo, sí es relevante que el atacante haya sopesado toda la información que razonablemente podía obtener y que la haya utilizado de manera razonable, en función de sus expectativas.[250] Esto debe incluir la posible actualización de la información disponible.

La ventaja militar concreta y directa excluye cualquier otro tipo de ventaja que no tenga conexión con lo militar:[251] política, psicológica, económica, financiera, social o moral.

---

[247] *Idem*.

[248] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, "*International humanitarian law and cyber operations during armed conflicts: ICRC position paper*", Ginebra, Suiza, noviembre, 2019, págs. 7, 45 y 49.

[249] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 113, pág. 4765.

[250] Cfr. TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, Prosecutor vs. Stanislav Galic. Sentencia de fondo y opinión de 5 de diciembre de 2003. Caso No. IT-98-29-T, párr. 58.

[251] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, "*Cyber operations during armed conflict: the principle of proportionality*", *Op. Cit.*, pág. 2.

El hecho de que la ventaja deba ser concreta implica que los beneficios especulativos, hipotéticos o generales no están cubiertos por el “Principio de Proporcionalidad”. Asimismo, el requisito de que la ventaja deba ser directa conlleva una relación causal entre el ataque cibernético y la ventaja militar prevista. Así, la ventaja militar remota o que aparecería solamente después de mucho tiempo no es útil bajo el “Principio de Proporcionalidad”.[252]

Un ataque cibernético ilícito sería uno que cause daño colateral excesivo. Esta evaluación no implica un estándar únicamente cuantitativo, sino también cualitativo: se debe evaluar el daño esperado en relación con la ventaja militar esperada en las circunstancias que prevalecen al momento de planear el ataque. Esto implica que se debe evaluar el ataque como un todo y no cada acción por separado, es decir, si un ataque contempla operaciones militares tradicionales y cibernéticas, la ventaja obtenida se debe considerar en función de ambas operaciones, las cuales constituyen el ataque completo.[253]

Así, todas las consideraciones antes expuestas deben estar presentes al momento de analizar la proporcionalidad de un ataque.

3.2.3. Necesidad militar y humanidad

Todas las reglas del derecho internacional humanitario reflejan un balance cuidadoso entre los “Principios de Necesidad Militar y Humanidad”. Si una

[252] *Idem*; Cfr. GISEL, Laurent, The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law, S.N.E., ICRC, Canadá, 2016, págs. 18-19.
[253] Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Regla 113, pág. 473.

operación cibernética durante un conflicto armado no está prohibida por una regla específica del derecho internacional humanitario, aun así, debe cumplir con los principios en comento.[254]

El "Principio de Necesidad Militar" implica que una parte en un conflicto armado únicamente puede recurrir a los medios y métodos necesarios para alcanzar el propósito legítimo del conflicto:[255] debilitar las fuerzas militares del enemigo.

El "Principio de Humanidad" impone límites en los medios y métodos de guerra que se pueden emplear, así como requiere que los combatientes que caigan en manos del enemigo deben ser tratados humanamente en todo momento. Su propósito es limitar el sufrimiento, las lesiones y la destrucción durante los conflictos armados, a la vez que proteger la vida, la salud y asegurar el respeto por el ser humano.[256]

El balance entre necesidad militar y humanidad debe ser aplicado incluso en las circunstancias más extremas y a través de un equilibrio cuidadoso y pragmático[257]

Una expresión de la interacción entre estos principios se encuentra en la prohibición de atacar instalaciones médicas —artículo 12 del "Protocolo Adicional

---

[254] Cfr. MACÁK, Kubo y RODENHÄUSER, Tilman, "Cyber operations during armed conflict: the principles of humanity and necessity", en Comité Internacional de la Cruz Roja, Ginebra, Suiza, 7 de marzo de 2023, pág. 1, [en línea] https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf.

[255] *Ibidem*, pág. 2.

[256] *Idem*.

[257] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, *Op. Cit.*, pág. 80.

I a los Convenios de Ginebra"—.[258] Independientemente de las necesidades de la guerra, el "Principio de Humanidad" es el fundamento de las provisiones que reducen dramáticamente la posibilidad de confiar en la necesidad militar para justificar un ataque a instalaciones médicas.

Una ventaja de las operaciones cibernéticas es que puede habilitar al personal militar para alcanzar sus objetivos sin dañar a la población civil o causar daño físico permanente a la infraestructura civil.[259]

Un ataque cibernético sofisticado podría consistir en fragmentos de códigos maliciosos que permanecen latentes durante semanas, meses o incluso años en diversos sistemas de todo el mundo y que, activados por un determinado comando o acontecimiento, como la movilización de tropas en un país enemigo, se reúnen en un objetivo predeterminado donde el programa maligno despliega su función destructiva o manipuladora. A esto se le conoce como bomba lógica.[260]

En ese tenor, las operaciones cibernéticas pueden servir tanto para causar daños considerables a la contraparte beligerante como para aminorar los efectos perniciosos y aun así conseguir efectivamente el propósito de cada parte: inhabilitar a las fuerzas armadas contrarias y vencer en el conflicto armado.

Así, cualquier tipo de operación militar que sea dirigida en el contexto de un conflicto armado y que se configure como un ataque en términos del derecho

---

[258] Cfr. HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, *Op. Cit.*, Regla 1, pág. 3; Cfr. SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, *Op. Cit.*, Reglas 131 y 132, págs. 513 y 515.

[259] Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, *Op. Cit.*, pág. 26.

[260] Cfr. GEISS, R. y LAHMANN, H., "*Cyber warfare: applying the principle of distinction in an interconnected space*", *Op. Cit.*, pág. 385.

internacional humanitario está regulada por el balance entre los “Principios de Necesidad Militar y Humanidad”.

3.3. Conclusiones

Derivado del análisis de las reglas del derecho internacional humanitario que se aplican a los medios y métodos de guerra cibernéticos, se concluye que:

- El artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra” implica un mecanismo de revisión *ex ante* sobre la licitud del empleo de medios o métodos de guerra cibernética en el contexto de un conflicto armado, el cual exige asegurar la legalidad del empleo del medio o método en cuestión desde su etapa más temprana de desarrollo.
- Los principios reguladores del derecho internacional humanitario, *id est*, distinción, proporcionalidad, necesidad militar y humanidad regulan cualquier operación cibernética que se configure como un ataque cibernético.
- Los elementos esenciales que dieron lugar a todas las reglas específicas del derecho internacional humanitario regulan también los medios y métodos de guerra cibernética.

Capítulo 4. Un nuevo instrumento jurídico para afirmar la aplicación de los principios reguladores del derecho internacional humanitario en la ciberguerra

En los capítulos anteriores se sentaron las bases de la aplicación del derecho internacional humanitario a la ciberguerra y cómo debe operar. Ahora, corresponde abordar la pertinencia de crear un instrumento jurídico sobre la regulación de la ciberguerra y qué contenido sería el idóneo.

Este capítulo se divide en cinco apartados. En primer lugar, se analizan las posturas y propuestas de instrumentos jurídicos que han expresado el Comité Internacional de la Cruz Roja, el Consejo Europeo y distintos doctrinarios. En segundo lugar, se explican las ventajas de los llamados instrumentos *soft law* de frente a los instrumentos *hard law*, con la finalidad de dilucidar qué tipo de instrumento es más pertinente para el caso de la regulación de la ciberguerra.

En tercer lugar, se abordará el instrumento jurídico que se propone y el contenido que se considera adecuado para regular el derecho internacional humanitario aplicado a la ciberguerra. En cuarto lugar, se presentará la propuesta concreta del instrumento jurídico que se plantea como el apropiado para regular la ciberguerra, como resultado último de todo lo expuesto a lo largo del presente trabajo. En quinto lugar, se puntualizan las conclusiones de este capítulo.

4.1. Posturas y propuestas de instrumentos jurídicos para regular la ciberguerra

El propósito de esta sección es exponer las posturas y propuestas relevantes sobre la creación de un nuevo instrumento jurídico internacional para regular la ciberguerra. Asimismo, se realizarán breves comentarios sobre la pertinencia de cada una. Esto servirá para nutrir la propuesta de esta tesis y diferenciarla claramente de propuestas anteriores.

4.1.1. Postura de expertos convocados por el Comité Internacional de la Cruz Roja

En 2018, el Comité Internacional de la Cruz Roja organizó una reunión de científicos y expertos en ciberseguridad. Estos expertos concluyeron que, como parte de las medidas a largo plazo para asegurar que las operaciones cibernéticas no contravinieran el derecho internacional humanitario, era pertinente la creación de un tratado, ya sea para prohibir estas operaciones o para regularlas. Incluso se mencionó la negociación de un cuarto protocolo adicional a los Convenios de Ginebra.[261]

Asimismo, a nivel técnico, en la misma conferencia se propusieron ciertas medidas: segregar la infraestructura civil de la militar; etiquetar los *softwares* maliciosos para evitar que escalen; desarrollar marcas de agua para identificar actores y objetos protegidos; y, medidas para evitar que el propósito de un

[261] Cfr. GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, *Op. Cit.*, pág. 39.

programa maligno pueda ser modificado.[262] Todas estas medidas podrían ser consideradas por los Estados en el desarrollo de sus operaciones.

Igualmente, se planteó la posibilidad de marcar objetos protegidos como sistemas, computadoras y otros dispositivos. Esta medida consistiría en una marca de agua digital para identificar actores o infraestructura protegida. En el caso de los primeros, se incluirían, por ejemplo, organizaciones civiles; mientras que, en el caso de los segundos, se consideraría la inclusión de infraestructura esencial y hospitales.[263]

De igual forma, se sugirieron ciertas vías de acción de frente a la aplicación del derecho internacional humanitario a las operaciones cibernéticas: 1) asegurar el respeto por el derecho internacional humanitario como existe; 2) clarificar el entendimiento de las restricciones y limitantes impuestas por el derecho internacional humanitario actual; 3) acordar o reafirmar las prohibiciones que impone el derecho internacional humanitario, como ataque a infraestructura civil esencial, al *internet* y otros sistemas que tendrían efectos globales, a procesos o infraestructura electoral y equipos de respuesta a emergencias informáticas; y, 4) prevenir la militarización del ciberespacio.

Al respecto, se considera que las propuestas de acciones específicas a nivel técnico y práctico no son apropiadas para ser incluidas en un instrumento jurídico que regule la ciberguerra, puesto que encajan mejor en el desarrollo de la aplicación de las normas del derecho internacional humanitario. Más bien, como se desarrollará a lo largo de este capítulo, se prefiere que el instrumento

[262] *Ibidem*, pág. 40.
[263] *Idem*.

jurídico propuesto encarne aspectos generales que permitan a los Estados un relativamente amplio margen de acción, de tal forma que, con la práctica Estatal, se pueda nutrir paulatinamente la mejor forma de llevar a cabo la ciberguerra de conformidad con el derecho internacional humanitario.

4.1.2. Postura del Consejo Europeo

En 2013, el Consejo Europeo manifestó que el derecho internacional ya aplicaba al ciberespacio y que, por lo tanto, no convocaban a la creación de un nuevo instrumento legal para las cuestiones cibernéticas. El Consejo únicamente manifestó que el esfuerzo pendiente era asegurarse de que la aplicación de los instrumentos existentes fuera mantenida en el ciberespacio. En específico, se refirió a los tratados internacionales en materia de crimen cibernético, derecho internacional humanitario y derechos humanos.[264]

La postura del Consejo Europeo se considera adecuada en tanto que los principios reguladores del derecho internacional humanitario aplican al ciberespacio y que debe procurarse su aplicación, tal como deriva de su origen convencional y consuetudinario. Sin embargo, un nuevo instrumento jurídico podría servir para moldear la práctica estatal, lo cual se explicará más adelante.

4.1.3. Dr. Benjamin Mueller

[264] Cfr. CONSEJO DE LA UNIÓN EUROPEA, “Draft Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, Bruselas, 21 de junio de 2013, párr. 6.

El doctor Benjamin Mueller propone la creación de un instrumento jurídico internacional para regular los conflictos armados en el ciberespacio. En particular, refiere que se deben acordar definiciones comunes de uso de la fuerza cibernética, ataque y espionaje cibernéticos, así como establecer una obligación de asistencia mutua entre agencias estatales para abordar actos ilícitos en el ciberespacio.[265]

El doctor refiere que, como en otros casos en los que se han desarrollado nuevas armas o formas de hacer la guerra, la clave es crear reglas pragmáticas que funcionen, así como monitorear el cumplimiento a través de un mecanismo institucional permanente. En particular, menciona el "Tratado de No Proliferación Nuclear" como ejemplo de un instrumento jurídico que ha mostrado resultados positivos en cuanto a la reducción de la posesión de armas nucleares en el arsenal de los Estados.[266] Estos elementos propuestos por Mueller se consideran apropiados en función de que permitirían el desarrollo práctico de la aplicación del derecho internacional humanitario al ciberespacio.

Asimismo, El doctor Mueller refiere que los Estados suelen intentar actuar de conformidad con las obligaciones internacionales que contraen.[267] Esto lo menciona como base para reflexionar sobre la pertinencia de crear un instrumento legal que contemple las reglas aplicables a la ciberguerra.

---

[265] Cfr. MUELLER, B., "The laws of war and cyberspace on the need for a treaty concerning cyber conflict", en LSE IDEAS, 2014, https://www.jstor.org/stable/resrep45315, pág. 2.
[266] *Ibidem*, pág. 3.
[267] *Ibidem*, pág. 4.

El doctor refiere que sin un instrumento legal que colme las definiciones que menciona como necesarias, las operaciones en el ciberespacio se manejarán en un área del derecho relativamente gris. Esto debido a que, las operaciones cibernéticas pueden causar graves perjuicios aun sin provocar efectos físicos.[268]

En cuanto al ciber espionaje, argumenta que esta actividad no suele calificarse como ilícita, debido a su constante utilidad reconocida por los Estados.[269] Al respecto, no se estima necesario abordar el tema del espionaje. Esto toda vez que, si bien se puede llevar a cabo a través de operaciones cibernéticas, no es el aspecto más urgente, debido a que no constituye un ataque cibernético.

Igualmente, el doctor menciona que la atribución de las operaciones cibernéticas a los verdaderos actores no es realmente un problema por dificultades técnicas, sino que es un problema por la falta de cooperación entre Estados. Esto lo motiva a sugerir que el nuevo tratado que regule las operaciones cibernéticas debe contemplar una obligación de cooperación para poder rastrear el origen de las operaciones en el ciberespacio.[270] Aunque este aspecto es relevante, se considera que puede abordarse en un desarrollo posterior sobre la cooperación en esta materia.

Como ejemplo, el doctor Mueller refiere el ya existente “Convenio sobre la Ciberdelincuencia”, también conocido como el “Convenio de Budapest”. Este

[268] *Ibidem*, pág. 7.
[269] *Ibidem*, pág. 9.
[270] *Ibidem*, pág. 12.

instrumento vinculante busca sincronizar el derecho penal doméstico de los Estados parte con la finalidad de facilitar la cooperación transfronteriza. También prevé la existencia de una red de puntos de contacto que funciona a todas horas, así como prevé que los Estados deben preservar la evidencia de una operación cibernética, si otra parte lo solicita. Sin embargo, el Convenio no prevé un mecanismo para hacer cumplir las obligaciones de cooperación.[271]

Mueller considera que la necesidad de distinguir entre ataque armado, uso de la fuerza y operación de inteligencia en el ciberespacio deriva de lo fácil que se transita entre una y otra en las operaciones cibernéticas.[272] Al respecto, este trabajo ya distingue entre operaciones de ataque a redes informáticas y de explotación de redes informáticas. Aunque no aborda el significado de ataque armado y uso de la fuerza. Empero, esto último no se considera necesario, ya que en la aplicación del derecho internacional humanitario lo más relevante es distinguir cuándo se está de frente a medios y métodos de guerra cibernética, así como ataques cibernéticos.

Así, los aspectos más relevantes de la propuesta del doctor Benjamin Mueller se limitan a la pertinencia de crear un instrumento jurídico de contenido pragmático y con un mecanismo de monitoreo de cumplimiento, con la finalidad de permitir el desarrollo progresivo de la aplicación del derecho internacional humanitario al ciberespacio a través de la práctica Estatal. Todo esto mediante un instrumento jurídico oportuno que sirva de guía.

[271] *Ibidem*, pág. 13.
[272] *Ibidem*, pág. 16.

4.1.4. Dr. Rex Hughes

El doctor Rex Hughes menciona que la relación entre ciberguerra y las relaciones internacionales crece constantemente, lo que crea la necesidad de regular la actividad en el ciberespacio. Para esto, propone la creación de un régimen multilateral para regular la ciberguerra a nivel global.[273]

Rex enuncia a algunos Estados que han creado instituciones gubernamentales con el propósito de desarrollar capacidades en el ciberespacio. Entre estos se encuentran: Reino Unido, Corea del Sur, India, China, Rusia, Estados Unidos e Israel.[274]

Además, Hughes señala algunos eventos en particular: una operación cibernética iniciada por China en contra de una planta de energía eléctrica en California, que casi causó el cese de operaciones en 2001; la operación cibernética lanzada por Israel en contra del sistema de defensa aéreo de Siria, seguido de un bombardeo en territorio de este último en 2007; y, las operaciones cibernéticas atribuidas a Rusia en contra de diversos sistemas de Estonia y Georgia, en 2007 y 2008 respectivamente.[275] Con esto, busca evidenciar la necesidad de crear un régimen legal en torno a la ciberguerra.

Rex refiere que el propósito de un tratado multilateral sobre ciberguerra es regular este método de guerra y sus consecuencias a la luz de algunos principios

[273] Cfr. HUGHES, R., "*A treaty for cyberspace*", en International Affairs (Royal Institute of International Affairs 1944-), Vol. 86, 2010, pág. 524.
[274] *Ibidem*, págs. 528-533.
[275] *Ibidem*, págs. 528-529.

centrales del derecho de la guerra:[276] necesidad militar, distinción, proporcionalidad, armas indiscriminadas, perfidia y neutralidad.

Sobre necesidad militar, sostiene que los ataques deben dirigirse hacia objetivos militares con el propósito de obtener una ventaja militar, pero que el inconveniente en el ciberespacio es distinguir entre sistemas y propiedad militar y no militar.[277] En cuanto al "Principio de Distinción", menciona que en el ciberespacio es especialmente complejo distinguir combatientes de no combatientes, ya que los ataques se pueden iniciar de forma anónima o encubierta. Con respecto al "Principio de Proporcionalidad", dice que el reto fundamental es distinguir entre objetivos militares y no militares, pues dificulta la posibilidad de balancear la ventaja militar obtenida y el daño infligido.[278]

Sobre armas indiscriminadas, destaca que las armas cibernéticas con el potencial de causar daño grave más allá del objetivo original deben prohibirse, si causan efectos indiscriminados. Por ejemplo, el uso del *internet* público con el propósito de distribuir un programa maligno. Sin embargo, enuncia que el problema recae en definir qué constituye un arma cibernética.[279] Este último aspecto ya se abordó en este trabajo. En el tercer capítulo se analiza qué constituye un arma cibernética.

En cuanto a la perfidia, manifiesta que está prohibido tergiversar objetivos militares legítimos en objetivos no militares mediante engaños que los hagan parecer protegidos bajo el derecho de la guerra, *v.gr.* dar uso militar a una red

[276] *Ibidem*, págs. 536.
[277] *Idem*.
[278] *Ibidem*, págs. 537-538.
[279] *Ibidem*, págs. 538-539.

académica. Sobre esto, otra vez refiere que la cuestión principal es la identificación y autenticación de los objetivos.[280]

Respecto de la neutralidad, propone que este principio implica que los beligerantes no deben atacar un Estado neutral a cambio de la garantía de que ese Estado no apoyará a la parte contraria en el conflicto. Empero, mantiene que el inconveniente en su aplicación estriba en que las redes de comunicación están integradas de tal forma que sería prácticamente imposible distinguir entre el uso de la infraestructura de una red en territorio de un Estado neutral y la de uno no neutral. Por ejemplo, las operaciones cibernéticas que perjudicaron a Estonia en 2007 involucraron aproximadamente un millón de computadoras de 75 países.[281]

En particular, este trabajo coincide con la postura del doctor Rex Hughes en relación con la importancia de aplicar los principios centrales del derecho de la guerra al ciberespacio. Además, resulta evidente que el principal problema que identifica el doctor tiene que ver con la aplicación del “Principio de Distinción” en el ciberespacio. Sin embargo, este aspecto se relaciona más con el desarrollo de la práctica en las operaciones militares, como se expuso en la reunión de expertos de 2018 del Comité Internacional de la Cruz Roja.

Se considera que la relevancia de un nuevo instrumento jurídico que regule la ciberguerra consiste en afirmar la aplicación de los elementos esenciales del derecho internacional humanitario y guiar de forma general su aplicación, no en detallar cada aspecto y peculiaridad de las operaciones cibernéticas.

---

[280] *Ibidem*, págs. 539.
[281] *Ibidem*, págs. 539-540.

4.1.5. Mtro. Alexi Franklin

El maestro Alexi refiere que la mayoría de los tratados internacionales existentes podrían cubrir actividades en el ciberespacio, incluso la ciberguerra, pero que es necesario que esas actividades sean expresamente delineadas para que los Estados actúen de conformidad con acuerdos específicos y no adopten conductas bajo límites poco claros.[282]

Igualmente, menciona que, si bien los tratados no siempre llevan a resultados perfectos, sí pueden contribuir significativamente a la paz y seguridad internacional. Esto debido a que, su implementación, por más lenta que sea, plantea el camino a seguir.[283]

En camino a describir su propuesta, el maestro Alexi refiere tratados internacionales sobre otro tipo de armas con la finalidad de exponer qué puntos podría aplicar de forma análoga a la regulación de la ciberguerra. En ese tenor, el maestro aborda la “Convención sobre Armas Biológicas”, la “Convención sobre Armas Químicas”, el “Tratado sobre la No Proliferación de las Armas Nucleares”, la “Convención sobre la Prohibición de las Minas Antipersonal y su Destrucción”, la “Convención sobre Municiones en Racimo” y la “Convención sobre Ciertas Armas Convencionales”.

---

[282] Cfr. FRANKLIN, A., “*An International Cyber Warfare Treaty Historical Analogies and Future Prospects*”, en Journal of Law & Cyber Warfare, Vol. 7, Núm. 1, 2018, pág. 151.
[283] *Ibidem*, pág. 152.

Al respecto, concluye que ninguno de los instrumentos antes mencionados sirve de base suficiente para elaborar un instrumento jurídico que regule la ciberguerra. Sin embargo, de su revisión extrae la idea central de que el tratado que se forme debe contener términos abiertos a una amplia interpretación, de tal suerte que puedan ir a la par de los desarrollos tecnológicos. Por otro lado, El maestro Franklin refiere que el "Manual de Tallinn" constituye un punto de partida adecuado para el desarrollo del derecho internacional humanitario aplicable al ciberespacio.[284]

El maestro Alexi menciona dos inconvenientes respecto de la redacción de un tratado sobre ciberguerra:[285] 1) la dificultad para definir la atribución de las conductas desarrolladas en el ciberespacio, y 2) el peligro potencial de exponer fuentes y métodos de ciberataques. En consecuencia, Franklin propone que el instrumento jurídico en cuestión tenga reglas razonables que los Estados puedan aceptar.

Así, las características particulares que propone son:[286] 1) prohibir armas cibernéticas específicas, 2) prohibir actos específicos, y 3) plantear límites explícitos a las armas cibernéticas. Asimismo, refiere que la creación de un protocolo a la "Convención de Ciertas Armas Convencionales" que cubra la ciberguerra sería un primer paso importante y un mecanismo potencial para impulsar la voluntad internacional.

---

[284] *Ibidem*, págs. 153 y 161.
[285] *Ibidem*, pág. 161.
[286] *Ibidem*, pág. 162.

Se considera que el acercamiento del maestro Alexi Franklin al tema es oportuno, ya que toma en cuenta la necesidad de una regulación abierta y razonable que permita formar la base del desarrollo de la aplicación del derecho internacional humanitario al ciberespacio. Asimismo, las propuestas de prohibiciones y restricciones a las armas cibernéticas se consideran apropiadas. Esto debe llevarse a cabo de conformidad con los principios reguladores del derecho internacional humanitario.

De igual forma, la creación de un protocolo a la "Convención de Ciertas Armas Convencionales" se considera una propuesta loable. Sin embargo, más adelante se expondrá por qué debería preferirse un instrumento jurídico distinto a un tratado internacional.

4.1.6. Lic. Davis Brown

El abogado Davis Brown sostiene que es un error pensar que el derecho de la guerra existente puede regular perfectamente la ciberguerra, toda vez que esta última tiene diferencias significativas con la forma tradicional de hacer la guerra, entre las cuáles se encuentran dos paradigmas que se ven alterados:[287] 1) el cambio de armas cinéticas hacia armas informáticas, y 2) la creciente dependencia militar en civiles, así como objetos y actividades civiles.

[287] Cfr. BROWN, D. "*A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*", en Harvard International Law Journal, Vol. 47, Núm. 1, 2006, págs. 181-182.

Con base en lo anterior, argumenta que las reglas de la guerra cibernética deben apegarse a principios legales generales que estén de acuerdo con la estructura legal preexistente de los conflictos armados. También, menciona que las nuevas reglas no deben ser tan rígidas que impongan cargas irrazonables sobre el recurso a la guerra informática. Así, afirma que una declaración por parte de los Estados acerca del derecho aplicable a la guerra informática aliviaría la incertidumbre sobre su aplicación.[288]

En esa línea, propone utilizar el término "ataque informático", debido a que las actividades que pretende regular en la propuesta de tratado cubren sistemas informáticos como objeto, medio o soporte de un ataque. Manifiesta que las operaciones que no causan daño físico o afectan a alguna persona u objeto civil no clasifican como ataque informático, como el espionaje.[289] En ese entendido, los términos "ataque informático" y "ataque cibernético" se utilizarán indistintamente en esta sección, así como los términos "guerra informática" y "guerra cibernética".

El abogado Davis Brown sostiene que la guerra informática surgió como un método de hacer la guerra.[290] Sobre este punto, omite analizar la distinción entre medios y métodos de guerra, la cual también puede y debe aplicarse a la ciberguerra, como se analizó en el capítulo segundo.

Asimismo, opina que es necesario y apropiado que los mismos principios de derecho internacional que regulan los conflictos tradicionales sean aplicados

[288] *Ibidem*, pág. 182.
[289] *Ibidem*, págs. 187 y 189.
[290] *Ibidem*, pág. 197.

a la guerra informática:[291] distinción, necesidad militar, humanidad, proporcionalidad, caballería —cubre la prohibición de perfidia, *id est*, dar la apariencia de un objetivo militar no lícito— y neutralidad.

El abogado Brown divide el tratado que propone en 6 secciones:[292] general, artículos 1-3; distinción, artículos 4-17; reglas de la guerra, artículos 18-25; derechos de Estados no parte de un conflicto armado, artículos 26-30; cumplimiento, artículos 31-32; y, misceláneos, no propone artículos. A continuación, se aborda y se comenta la pertinencia del contenido de cada artículo.

En el primer artículo define 4 términos: ataque informático, uso de sistemas informáticos en un conflicto armado, Estado y derecho de los conflictos armados. Al respecto, se considera que resulta innecesario proveer la definición de los últimos dos términos, ya que su significado es provisto por el derecho internacional general.

En cuanto al uso de sistemas informáticos en un conflicto armado, menciona que " (…) significa uso de ordenadores y/u otros sistemas informáticos y comunicaciones en un ataque informático, en contraposición al uso con el único propósito de comunicación, recopilación de inteligencia, apoyo logístico, defensa pasiva de comunicación, defensa pasiva de redes informáticas u otras mejoras de la fuerza".[293]

---

[291] *Ibidem*, pág. 190.

[292] *Ibidem*, págs. 215-221.

[293] *Ibidem*, pág. 215: "...means the use of computers and/or other information and communications systems in an information attack, as opposed to use for the sole purpose of communication, intelligence gathering, logistical support, passive computer network defense, or other force enhancements."

Sobre la definición del uso de sistemas informáticos en un conflicto armado, se considera que es innecesaria. Esto es debido a que, la descripción que hace sobre cuándo debe considerarse que los sistemas informáticos se usan en un conflicto armado no es de utilidad para aplicar el derecho internacional humanitario. Es más relevante saber si los sistemas informáticos constituyen un medio o método de hacer la guerra que deba ser regulado por el derecho internacional humanitario, ya que es como opera este régimen.

Respecto de la definición de ataque informático, refiere que "(...) significa el uso de sistemas informáticos y/u otros sistemas de información o comunicaciones para destruir, alterar o manipular datos o imágenes, realizar ataques de denegación de servicio, transmitir códigos maliciosos o perpetrar ataques similares, o causar daños físicos a cualquier objetivo, con el fin de infligir lesiones o degradar la capacidad o voluntad de lucha del enemigo".[294]

En particular, la definición provista se excede en ejemplos. Es más útil proveer una definición amplia que derive del concepto de ataque en el derecho internacional humanitario, de tal suerte que pueda estar a la par del desarrollo tecnológico.

En el segundo artículo, el abogado Davis refiere que el tratado que propone regula el uso de sistemas informáticos en conflictos armados a través de la aplicación de los principios generales de distinción, necesidad militar,

[294] *Idem*: "...means the use of computer and/or other information or communications systems to destroy, alter, or manipulate data or images, engage in denial-of-service attacks, transmit malicious code, or perpetrate similar attacks, or do physical damage to any target, for the purpose of inflicting injury or degrading the enemy's ability or will to fight."

humanidad, proporcionalidad y caballería. Esto se considera apropiado, excepto el “Principio de Caballería”, lo cual se abordará más adelante.

En el tercer artículo, propone que un ataque que viola el derecho internacional humanitario a través de medios convencionales también viola el derecho internacional humanitario cuando se lleva a cabo a través de sistemas informáticos. Esta comparación es cierta, en tanto que una violación al derecho internacional humanitario es independiente de cómo suceda. Sin embargo, es un parangón poco ilustrador, si se toma en consideración que los efectos de la ciberguerra pueden ser muy distintos a los de la guerra convencional y aun así violar el derecho internacional humanitario.

Posteriormente, el abogado Brown aborda el término de combatiente en el artículo 4, pero no desarrolla alguna característica especial en función del ciberespacio. Por ende, se considera que dicho artículo es irrelevante, además porque la definición de combatiente es provista por el derecho internacional humanitario convencional y consuetudinario. De igual manera, parece innecesaria la definición de no combatiente que Davis refiere en el artículo 5, pues lo define como cualquier persona que no sea combatiente.

En consonancia, menciona en el artículo 6 que los civiles parte de un levantamiento en masa no serán considerados combatientes. Empero, esta especificación no tiene alguna relevancia particular en el contexto de la ciberguerra, pues no resulta necesario crear una nueva categoría de combatiente o no combatiente en función de la guerra cibernética, tal como se refirió en el párrafo anterior.

En el mismo sentido, es superflua la especificación que hace Davis en el artículo 7 sobre que solamente los combatientes tendrán permitido realizar ataques informáticos contra otros Estados. El derecho internacional humanitario, como existe actualmente, sirve para regular quiénes participan lícitamente en un conflicto, sin que sea necesario puntualizar alguna característica especial relativa al ciberespacio.

En el artículo 8, el abogado Davis Brown propone que los Estados solamente pueden realizar ataques informáticos en instalaciones ubicadas a una distancia segura de las instalaciones utilizadas por no combatientes. El contenido de este artículo es útil, pero incompleto. Como se describió en los capítulos anteriores, un ataque cibernético puede generar la pérdida de la funcionalidad de un sistema informático sin que se cree algún efecto pernicioso adicional, como sí sucedería en el caso de otros ataques cibernéticos que provocan la liberación de fuerzas peligrosas. Así, la distancia entre las instalaciones objetivo no es realmente un parámetro relevante.

El artículo 9 propone que los Estados separarán los sistemas informáticos usados por combatientes de los usados por no combatientes. Esto es poco factible, como se expuso en el capítulo tercero. Sin embargo, este artículo también plantea que los Estados no usen sistemas informáticos y datos que no sean un objetivo militar para encubrir sistemas informáticos que sí constituyan un objetivo militar. Esta parte de la propuesta es necesaria en función de aplicar el “Principio de Distinción” con respecto de las particularidades del ciberespacio.

En el artículo 10, el abogado Davis Brown propone que los ataques informáticos solamente deberían lanzarse desde sistemas informáticos operados

por combatientes, lo que contempla no utilizar sistemas informáticos distintos a los usados por combatientes como intermediarios para realizar el ataque. Esto podría incluir el uso de *botnets*, pues son dispositivos controlados remotamente a través de los cuales se realiza una operación cibernética dirigida al objetivo en cuestión, *v.gr.* una operación de denegación de servicio distribuido. Se considera que este artículo es apropiado

El artículo 11 plantea que los Estados que realicen ataques informáticos deberán esforzarse por minimizar los efectos adversos a los no combatientes, que es oportuno.

El artículo 12 refiere que los ataques informáticos que causen daños físicos deberán dirigirse hacia objetivos militares, a la vez que deberán observar el “Principio de Proporcionalidad”. El artículo 13 prohíbe los ataques informáticos que pueden dañar el medio ambiente. El artículo 14 prohíbe los ataques informáticos contra instalaciones que contienen fuerzas peligrosas. El artículo 15 habla de las instalaciones que no deben ser objeto de un ataque informático, como iglesias, hospitales, bancos, plantas eléctricas, centros de alimentos y agua, sistemas de comunicación y propiedad cultural. Estos cuatro artículos son apropiados, toda vez que derivan de la aplicación de los principios reguladores del derecho internacional humanitario, como se explicó en el capítulo tercero.

La propuesta del artículo 16 es que los Estados tomen todas las medidas razonables para asegurar que los ataques informáticos que contengan códigos maliciosos discriminen entre sistemas informáticos usados por combatientes y no combatientes. En el artículo 17 menciona que los Estados deben programar las bombas lógicas para neutralizarse a sí mismas de forma automática después de

haber cumplido su objetivo. Estos dos artículos abordan especificaciones idóneas respecto de ataques informáticos de acuerdo con los principios del derecho internacional humanitario, especialmente distinción.

El abogado Davis Brown refiere en el artículo 18 que los Estados deberían conducir la guerra informática de acuerdo con los principios consuetudinarios de necesidad militar, proporcionalidad, humanidad y caballería, que transpone adecuadamente los principios relevantes en todo tipo de guerra.

En los artículos 19 a 22, se plantea la prohibición de ciertas conductas que, aunque importantes, no son las más relevantes en un instrumento que recién pretende regular la ciberguerra. El abogado Brown propone prohibir transacciones financieras o comerciales fraudulentas, las interferencias en las finanzas personales de cualquier persona, el robo de identidad y contactar con personas no combatientes para causarles terror.

El planteamiento del artículo 23 es que el uso de sistemas informáticos para hacer creer al adversario que una persona, una ubicación, o una instalación está protegida bajo el derecho internacional humanitario, con el propósito de abusar de esa creencia, es un acto de perfidia y está prohibido. Esta provisión es adecuada, pues una conducta contraria también afectaría al "Principio de Distinción".

El artículo 24 refiere que los Estados no deberían transmitir código malicioso disfrazado de mensajes inocuos si los mensajes simulan provenir de un Estado distinto al Estado atacante o al Estado atacado, o si el mensaje simula provenir de una persona o institución que tiene estatus protegido. Este artículo transpone oportunamente la aplicación de los “Principios de Distinción y

Neutralidad", pues indica que el uso de esos códigos maliciosos debe ser entre las partes en conflicto.

Asimismo, en el artículo 25, el abogado Davis Brown propone la prohibición de la alteración de imágenes o grabaciones que induzcan a creer que un acto ilícito, un crimen de guerra o un ataque de un Estado contra un tercer Estado han ocurrido cuando en realidad no han sucedido. Este artículo aborda un aspecto relacionado con el uso de información para engañar al enemigo, más que operaciones cibernéticas que involucran afectaciones a redes informáticas. Por ende, esta provisión se pone fuera de consideración para el presente trabajo.

La propuesta del artículo 26 es que los Estados no deberán realizar ataques informáticos contra Estados neutrales, así como estos últimos no deberán apoyar de forma alguna la realización de ataques informáticos contra los Estados beligerantes. Este artículo se considera innecesario, en función de que, en general, la conducción de las hostilidades debe realizarse entre las partes beligerantes, no así contra Estados neutrales. Esto no requiere una especificación particular en torno al ciberespacio. Lo relevante es que, si un ataque cibernético es equiparable a un ataque tradicional, entonces no debe dirigirse hacia un Estado neutral, como consecuencia natural de que los dos tipos de ataques son equiparables.

En el artículo 27, el abogado Davis Brown propone que los Estados no conduzcan actividades de guerra informática en la jurisdicción de otro Estado, que incluiría usar los nombres de dominio y los sistemas informáticos, a menos que el otro Estado otorgue su consentimiento. El artículo 28 adiciona que los Estados no deberán lanzar ataques informáticos desde sistemas informáticos en

Estados neutrales o tomar el control de esos sistemas para realizar ataques informáticos.

Sobre los dos artículos anteriores, se considera que deben complementarse con la idea de que el uso de los sistemas informáticos o de la infraestructura de otros Estados únicamente está permitida cuando sea como vía de paso. Es decir, debería prohibirse únicamente que los ataques informáticos se hagan desde Estados neutrales, pero no que el tráfico de datos transite por su infraestructura.

El artículo 29 refiere que los sistemas informáticos y líneas de comunicación en Estados neutrales no deberán ser objeto de un ataque informático, ni siquiera si se usan como conducto para un ataque informático, a menos que el Estado neutral activamente preste apoyo para realizar el ataque. Al respecto, aplican las mismas consideraciones previas en cuanto a la aplicación de las normas de neutralidad en la ciberguerra.

De igual manera, en el artículo 30 se plantea que los Estados neutrales no tendrán la obligación de cortar comunicación o vínculos de *internet* con los Estados beligerantes, pero que podrán hacerlo si su neutralidad es violentada por esos Estados. Este artículo propone una situación interesante en el contexto de la ciberguerra, pero excede los elementos esenciales de su regulación e incluso podría resultar poco factible, debido a la relevancia de la interconectividad en distintos ámbitos hoy día.

Los artículos 31 y 32 se refieren a las medidas para promover el cumplimiento de la parte sustantiva del tratado propuesto, como emitir legislación nacional y conceder jurisdicción a la Corte Internacional de Justicia sobre

disputas respecto de la aplicación del tratado. Sin embargo, su contenido está fuera del ámbito de este trabajo. Son disposiciones innecesarias en un primer instrumento que pretende regular la ciberguerra.

En conclusión, el abogado Brown acierta al decir que sería un error pensar que el derecho internacional humanitario puede regular perfectamente la ciberguerra, debido a las características específicas de esta última. Por lo que, es relevante promover el desarrollo paulatino de este régimen jurídico sobre la regulación de la guerra cibernética. Asimismo, es oportuno que considere que deben aplicarse los elementos esenciales del derecho internacional humanitario.

De igual manera, este trabajo coincide con la idea de que una declaración por parte de los Estados acerca del derecho aplicable a la ciberguerra aliviaría la incertidumbre sobre su aplicación. Aunque al final el abogado Brown propone un tratado.

Posteriormente se retomarán los aspectos que se consideran apropiados de esta propuesta.

4.2. Conveniencia de crear un instrumento *soft law* sobre el derecho internacional humanitario aplicable al ciberespacio

En el apartado anterior se revisaron las propuestas de instrumentos jurídicos para regular el derecho internacional humanitario aplicable al ciberespacio. Éstas proponen la creación de un tratado —usualmente reconocido como instrumento *hard law*—, incluso hay quienes mencionan que se debería crear un tratado en

conexión con otros ya existentes, como los Convenios de Ginebra de 1949 o la Convención sobre Ciertas Armas Convencionales.

Sin embargo, ninguna de las propuestas aborda las ventajas y desventajas de los posibles instrumentos que pueden contener las normas relevantes respecto de la regulación de la ciberguerra. Sobre el particular, este trabajo considera apropiado exponer las ventajas de los instrumentos *soft law* de frente a los instrumentos *hard law*. Esto con la finalidad de saber qué tipo de instrumento es más conveniente.

Actualmente hay órganos especializados en el desarrollo del derecho internacional que abordan el tema de los instrumentos *soft law* debido al aumento constante de su relevancia en las relaciones internacionales. Al respecto, se señala a la Comisión de Derecho Internacional de la Organización de las Naciones Unidas, el Comité de Asesores Jurídicos sobre Derecho Internacional Público del Consejo de Europa, y el Comité Jurídico Interamericano de la Organización de los Estados Americanos.

En cuanto a la Comisión de Derecho Internacional, ésta decidió, el año pasado, incluir el tema “Los acuerdos internacionales jurídicamente no vinculantes” en su programa de trabajo a largo plazo.[295] Entre las razones para su inclusión destaca la creciente atención que la práctica estatal les refiere, así como su notable relación con el desarrollo del derecho internacional

[295] Cfr. COMISIÓN DE DERECHO INTERNACIONAL, “Informe de la Comisión de Derecho Internacional”, Documento de Naciones Unidas A/77/10, 18 de abril a 3 de junio y 4 de julio a 5 de agosto de 2022, Anexo 1.

consuetudinario, debido a que estos instrumentos pueden expresar los elementos constitutivos de la costumbre internacional.

Respecto del Comité de Asesores Jurídicos sobre Derecho Internacional Público, el tema en comento figura en su programa desde 2021. En un principio, este comité trató el tema únicamente desde una perspectiva doctrinal,[296] mediante la realización de eventos con expertos en el tema.

Sin embargo, recientemente se volcó hacia la práctica de los Estados —22 en este caso—, que derivó el siguiente hallazgo:[297] la mayoría de los Estados sostuvieron que los instrumentos jurídicamente no vinculantes pueden, bajo ciertas circunstancias, producir efectos jurídicos indirectos, como constituirse en una guía interpretativa o facilitar la posterior conclusión de acuerdos vinculantes. Además de que es más fácil concluir un acuerdo no vinculante.

Sobre el Comité Jurídico Interamericano, en su trabajo "Directrices del Comité Jurídico Interamericano para los Acuerdos Vinculantes y no Vinculantes"[298] trató de aclarar las definiciones de los acuerdos vinculantes y no vinculantes, los métodos para identificarlos, la capacidad para concertarlos y sus efectos jurídicos.

Empero, los trabajos antes referidos no se acercan lo suficiente a los instrumentos del mismo tipo al que se propone en este trabajo, o bien no han

---

[296] Cfr. COMITÉ DE ASESORES JURÍDICOS SOBRE DERECHO INTERNACIONAL PÚBLICO, Expert Workshop on "Non-Legally Binding Agreements in International Law", Conferencia en línea, 26 de marzo de 2021.

[297] Cfr. ZIMMERMANN, Andreas, "The practice of States and International Organisations regarding non-legally binding agreements", informe para el Comité de Asesores Jurídicos sobre Derecho Internacional Público (CAHDI), Estrasburgo, Francia, 23 de marzo de 2023, páginas 5-6.

[298] Cfr. COMITÉ JURÍDICO INTERAMERICANO, "Directrices del Comité Jurídico Interamericano para los Acuerdos Vinculantes y no Vinculantes", Washington DC, 1 de noviembre de 2020.

llegado a desarrollar ese aspecto aún. Consecuentemente, el trabajo de los órganos especializados antes mencionados sirve más bien como un indicador de la creciente valía de los instrumentos *soft law*.

Ahora bien, en lo subsecuente se abordarán las diversas ventajas y desventajas de los instrumentos *soft* y *hard law*, con miras a resaltar la conveniencia de un tipo muy particular de instrumento: resoluciones de la Asamblea General de las Naciones Unidas que contienen declaraciones sobre un determinado régimen del derecho internacional.

Las ventajas del *hard law* son:[299] 1) permite a los Estados comprometerse de forma creíble; 2) los instrumentos son confiables, puesto que tienen efectos legales directos en las jurisdicciones nacionales; y, 3) permite un mejor monitoreo y cumplimiento de las obligaciones contraídas, toda vez que suelen incluir un mecanismo de solución de controversias. Sin embargo, el cumplimiento de los instrumentos *soft law* no está *per se* condenado a una débil voluntad de cumplimiento por parte de los Estados; más bien, esto depende de otros elementos.

El cumplimiento de normas *soft law* se relaciona con cuatro factores:[300] 1) el contexto en el que surgió la norma, *id est*, si surge en relación con un instrumento *hard law* o si emerge independientemente; 2) el contenido y precisión de las normas; 3) apoyo institucional, como la existencia de mecanismos de revisión; y, 4) el tipo de actores y el alcance de cooperación que se requieren

[299] Cfr. SHAFFER, G. y POLLAK, M., "*Hard and Soft Law"*, en DUNOFF, J. y POLLAK, M. (eds.), Interdisciplinary Perspectives on International Law and International Relations: The State of the Art, S.N.E., Cambridge University Press, Reino Unido, 2012, pág. 203.
[300] *Ibidem*, pág. 215.

para cumplir los objetivos de la norma, por ejemplo, es más sencillo cuando solamente se requiere la voluntad de los Estados que cuando se requiere de la interacción con actores privados.

Hay tres características que usualmente se asocian a un instrumento *soft law*:[301] no es vinculante; consiste en normas generales o principios, no reglas; y, no se puede hacer cumplir a través de resoluciones vinculantes de disputas.

El primer elemento implica que los tratados son *hard law* y todos los demás instrumentos no vinculantes son *soft law*. Sin embargo, el profesor Alan Boyle refiere que la distinción entre instrumentos *hard* y *soft law* no es tan definida como referir que los tratados son parte del primero y cualquier otro acuerdo no vinculante es parte del segundo. Más bien, la naturaleza jurídica de los instrumentos puede transitar entre ambas clasificaciones.[302]

En cuanto a la segunda característica, ésta implica que los instrumentos *hard law* tienen obligaciones claras y razonablemente específicas, expuestas en forma de reglas. Mientras que, los instrumentos *soft law* tienen normas o principios de carácter general en su contenido y fraseo. Esta distinción conlleva a que los tratados sean considerados tanto *soft* como *hard law*, toda vez que el elemento decisivo es el contenido de las provisiones del instrumento en cuestión.[303]

Sobre la tercera característica, ésta es tan simple como referir que los instrumentos cuyo cumplimiento pueda ser sujeto a un proceso de adjudicación

---

[301] Cfr. BOYLE, Alan, "*Some Reflections on the Relationship of Treaties and Soft Law*", en The International and Comparative Law Quarterly, Vol. 48, Núm. 4, 1999, págs. 901-902.
[302] *Ibidem*, pág. 901.
[303] *Ibidem*, págs. 901-902.

vinculante serán reconocidos como *hard law*. Es decir, todo depende del carácter del proceso de solución de disputas asociado con el instrumento.[304] De esta manera, un instrumento que ni siquiera contempla un proceso de solución de controversias sobre la aplicación de éste debería ser considerado *soft law*.

Se puede decir que los instrumentos *soft law* tienen al menos un elemento de compromiso de buena fe, un deseo de influenciar la práctica estatal y un elemento de crear derecho, así como contribuir al desarrollo progresivo de este último. En ese entendido, este tipo de instrumentos son una alternativa o parte del proceso de creación de tratados multilaterales.[305]

Los instrumentos *soft law* representan una alternativa loable de frente a los instrumentos *hard law* por las siguientes razones:[306] 1) es más fácil alcanzar un acuerdo con disposiciones detalladas cuando el instrumento no es vinculante, toda vez que las consecuencias del incumplimiento son limitadas; 2) es más fácil adherirse a instrumentos no vinculantes, pues para algunos Estados esto permite evitar procesos internos de ratificación; 3) es más fácil hacer modificaciones a estos instrumentos que a tratados; y, 4) constituyen evidencia del apoyo y consenso internacional respecto del tema en cuestión, además de que no suelen estar sujetos a reservas ni a la necesidad de esperar por la ratificación y entrada en vigor.

Asimismo, la flexibilidad de los instrumentos *soft law* permite que los Estados experimenten con su aplicación bajo un leve compromiso de la

[304] *Ibidem*, pág. 902.
[305] *Idem*.
[306] *Ibidem*, págs. 902-903

soberanía en áreas sensibles. Los Estados tienen más voluntad para comprometerse en esfuerzos de cooperación ambiciosos a través de instrumentos no vinculantes. Esto permite que los Estados aprendan mientras implementan el instrumento en la medida en que lo consideran pertinente, lo cual se ve enriquecido con sistemas de revisión de su implementación.[307]

En 1999, el profesor Alan Boyle mencionó que el proyecto de articulado sobre responsabilidad Estatal de la Comisión de Derecho Internacional podría ser codificado a través de una resolución de la Asamblea General de Naciones Unidas o de una declaración intergubernamental.[308] Hoy día, el proyecto antes referido lleva más de 20 años de haber sido concluido[309] y reconocido por la Asamblea General[310] en una resolución en la que tomó nota del proyecto.

Actualmente, el proyecto de responsabilidad estatal no constituye un instrumento vinculante. Sin embargo, a través de la continua referencia a este instrumento por parte de la práctica Estatal y por resoluciones de cortes y tribunales internacionales, se ha reconocido que diversas disposiciones del proyecto son vinculantes.[311] Esto muestra que, en verdad, los instrumentos *soft*

---

[307] Cfr. SHAFFER, G. y POLLAK, M., "*Hard and Soft Law"*, *Op. Cit.*, págs. 204 y 215.

[308] Cfr. BOYLE, Alan, "*Some Reflections on the Relationship of Treaties and Soft Law*", *Op. Cit.*, pág. 903.

[309] Cfr. ORGANIZACIÓN DE LAS NACIONES UNIDAS, COMISIÓN DE DERECHO INTERNACIONAL, "State responsibility", en Analytical Guide to the Work of the International Law Commission, Ginebra, 2023, [en línea] https://legal.un.org/ilc/guide/9_6.shtml.

[310] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Responsabilidad del Estado por hechos internacionalmente ilícitos", Resolución 56/83, Quincuagésimo sexto período de sesiones, 28 de enero de 2002.

[311] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Compilación de las decisiones de cortes, tribunales y otros órganos internacionales", Documento de Naciones Unidas A/77/74, Septuagésimo séptimo período de sesiones, 29 de abril de 2022; Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Compilación de las decisiones de cortes, tribunales y otros órganos internacionales", Documento de Naciones Unidas A/74/83, Septuagésimo cuarto período de sesiones, 23 de abril de 2019.

law pueden servir de base para el desarrollo del derecho internacional y generar derecho vinculante.

El contenido de los instrumentos *soft law* se puede transformar en *hard law* en dos situaciones:[312] si su contenido se consagra en un instrumento *hard law* posteriormente o si la *inveterata consuetudo* —práctica estatal— y la necesaria *opinio iuris sive necessitatis* —convicción sobre la necesidad de cumplir con un deber jurídico— transforma su contenido en costumbre.

Los instrumentos *soft law* moldean la práctica internacional y esto sirve para dar forma al derecho vinculante. De tal suerte, los compromisos políticos pueden volverse obligaciones legales.[313]

Tratados e instrumentos *soft law* pueden generar la concentración de consenso sobre reglas y principios, con la finalidad de movilizar una respuesta Estatal consistente y general. En ese sentido, la interacción entre *soft* y *hard law* también permite que los instrumentos del primer tipo sirvan:[314] 1) de base para la subsecuente creación de un tratado multilateral, o 2) como mecanismos de interpretación autoritativa o amplificación de los términos de un tratado.

La Declaración Universal de Derechos Humanos es un buen ejemplo de un instrumento *soft law* con la capacidad de influenciar el desarrollo de *hard law*. Después de la adopción de esta declaración por la Asamblea General de

---

[312] Cfr. OLIVIER, Michele, "*The relevance of 'soft law' as a source of international human rights*", en The Comparative and International Law Journal of Southern Africa, Vol. 35, Núm. 3, 2002, pág 295.
[313] Cfr. BOTHE, Michael, "*Legal and Non-Legal Norms - a meaningful distinction in international relations?*", en Netherlands Yearbook of International Law, Vol. 11, 1980, pág. 79.
[314] Cfr. SHAFFER, G. y POLLAK, M., "*Hard and Soft Law"*, *Op. Cit.*, pág. 208; Cfr. BOYLE, Alan, "*Some Reflections on the Relationship of Treaties and Soft Law*", *Op. Cit.*, págs. 904-905.

Naciones Unidas,[315] surgieron tratados vinculantes que reflejaron los derechos humanos contenidos en la declaración, seguido de la creación de la maquinaria para su implementación.[316]

Asimismo, algunas de las resoluciones más famosas de la Asamblea General de Naciones Unidas permiten entrever que éstas forman parte importante del impulso al desarrollo del derecho internacional.[317] Por ejemplo, la "Resolución 3314 (XXIX) 'Definición de la agresión'"[318] y "Resolución 1514 'Declaración sobre la concesión de la independencia a los países y pueblos coloniales'",[319] que constituyeron la base para el avance en el entendimiento de qué constituye un ataque armado y el derecho a la autodeterminación.

Respecto de la "Resolución 3314", la Corte Internacional de Justicia ha considerado que su artículo 3, párrafo g), refleja costumbre internacional, en relación con el entendimiento sobre lo que configura un ataque armado.[320] En cuanto a la Resolución 1514", ésta fue, junto con la Carta de las Naciones Unidas, el punto de partida desde el cual la misma corte consideró la evolución del

[315] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Declaración Universal de Derechos Humanos", Resolución 217 A (III), Centésimo octogésimo tercera sesión plenaria, 10 de diciembre de 1948.
[316] Cfr. OLIVIER, Michele, "*The relevance of 'soft law' as a source of international human rights*", *Op. Cit.*, pág. 298.
[317] Cfr. GUTIÉRREZ BAYLÓN, Juan de Dios, Sistema jurídico de las Naciones Unidas, S.N.E., Editorial Porrúa, México, D.F., 2007, pág. 80.
[318] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Definición de la agresión", Resolución 3314 (XXIX), Vigésimo noveno período de sesiones, 14 de diciembre de 1974.
[319] Cfr. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Declaración sobre la concesión de la independencia a los países y pueblos coloniales", Resolución 1514 (XV), Décimo quinto período de sesiones, 14 de diciembre de 1960.
[320] Cfr. CORTE INTERNACIONAL DE JUSTICIA, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Estados Unidos de América), *Op. Cit*., pág. 103, párr. 195.

derecho a la autodeterminación en la opinión consultiva "*Consecuencias jurídicas de la separación del archipiélago de Chagos de Mauricio en 1965*".[321]

Adicionalmente, la Corte Internacional de Justicia ha reconocido que las resoluciones de la Asamblea General pueden servir para probar la existencia de una regla o el surgimiento de la *opinio juris* respecto del tema en cuestión. Esto sujeto al contenido de la resolución, las condiciones de su adopción, su carácter normativo y las demás resoluciones relacionadas que muestren la evolución de la *opinio juris*.[322]

La Asamblea General, como uno de los órganos principales de Naciones Unidas,[323] es el único en el que están representados todos los Estados miembros. Esto "la convierte consecuentemente en el mayor foro político de la comunidad internacional".[324] Así, sus resoluciones "representan en el menor de los casos una expresión de *lex ferenda* que puede ser consultada *a posteriori* como referente casi matemático de la evolución del derecho internacional".[325] En ese entendido, las resoluciones de este órgano onusiano[326] son un medio idóneo para sentar la base del desarrollo de, por ejemplo, el derecho internacional humanitario aplicado al ciberespacio.

---

[321] Cfr. CORTE INTERNACIONAL DE JUSTICIA, Legal Consequences of the Separation of the Chagos Archipielago from Mauritius in 1965. Opinión Consultiva de 25 de febrero de 2019. I.C.J. Reports 2019, pág. 130, párr. 142.

[322] Cfr. CORTE INTERNACIONAL DE JUSTICIA, Legality of The Threat or Use of Nuclear Weapons, *Op. Cit.*, págs. 254-255, párr. 70.

[323] Cfr. "Carta de las Naciones Unidas", San Francisco, Estados Unidos de América, 25 de junio de 1945, D.O.F. 17 de octubre de 1945, art. 7.

[324] GUTIÉRREZ BAYLÓN, Juan de Dios, Sistema jurídico de las Naciones Unidas, *Op. Cit.*, pág. 65.

[325] *Ibidem*, pág. 79.

[326] Este término fue adoptado por el Dr. Juan de Dios Gutiérrez Baylón en su libro sobre el sistema jurídico de las naciones unidas. Onusiano hace referencia a algo que procede de o pertenece a la Organización de las Naciones Unidas, tal como puede colegirse del significado del sufijo -ano.

Es así como, un instrumento jurídico vinculante, como un tratado, no es imprescindible para dar un paso importante en la regulación del derecho internacional humanitario aplicado a la ciberguerra. Es más, insistir en la creación de un tratado podría retrasar la adopción de un instrumento jurídico sobre este tema. Es por eso que, este trabajo propone la creación de un instrumento jurídico *soft law* que permita a los Estados experimentar con la aplicación del derecho internacional humanitario en la conducción de las hostilidades mediante operaciones cibernéticas.

4.3. Forma y contenido idóneo de un nuevo instrumento jurídico para regular la ciberguerra

Este trabajo propone la creación de una declaración que sea adoptada, mediante una resolución, por la Asamblea General de Naciones Unidas. El propósito es que este instrumento *soft law* se constituya en una expresión clara de la voluntad estatal de aplicar el derecho internacional humanitario al ciberespacio.

Las resoluciones son expresiones formales de la opinión o voluntad de los órganos de Naciones Unidas. Estas resoluciones, generalmente, tienen dos partes claramente diferenciadas: un preámbulo y una parte operativa. El preámbulo contiene las consideraciones sobre las cuales la acción es tomada, ya sea una opinión expresada o una directriz dada. Mientras que, la parte operativa declara la opinión del órgano o la acción a ser ejecutada.[327]

[327] Cfr. DEPARTAMENTO DE SERVICIOS DE CONFERENCIAS, “United Nations Editorial Manual”, Documento de Naciones Unidas ST/DCS/2, Estados Unidos, 1983, pág. 167.

La resolución que se propone en este trabajo se redactó sobre la base del manual editorial de Naciones Unidas, que indica la forma de elaborar resoluciones de la Asamblea General.

En ese tenor, se considera que el contenido de dicha resolución y la declaración que contiene debe ser de conformidad con el análisis y las conclusiones alcanzadas en el presente trabajo.

Es preciso definir los conceptos que necesariamente se emplean cuando se habla de la guerra cibernética, como: ciberespacio, red informática, infraestructura cibernética, operaciones cibernéticas, ciberguerra, ataque cibernético, medio y método de guerra cibernética.

La declaración deberá reconocer la aplicación del derecho internacional humanitario al ciberespacio y a todos los tipos de conflictos armados, así como a todos los medios y métodos de guerra. Todo esto independientemente de las tecnologías empleadas. Es decir, el punto crucial es reconocer que, aunque el derecho convencional no regula explícitamente la ciberguerra, los Estados reconocen la extensión del derecho internacional humanitario sobre esta última.

Es importante que el instrumento en cuestión haga referencia al carácter consuetudinario de los principios reguladores del derecho internacional humanitario, así como a la obligación contenida en el artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra”. Así, declaración también servirá para reforzar la obligación de revisión de los medios y métodos de guerra nuevos.

Se deberá mencionar que la aplicación del artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra” cubre los medios y métodos de guerra cibernética. Sobre el particular, no es necesario elaborar más, toda vez que esta

obligación ya está en vigor para los Estados parte del “Protocolo Adicional I a los Convenios de Ginebra”. Sin embargo, es relevante mencionar que debe aplicarse en el contexto del ciberespacio para reforzar el consenso internacional sobre su aplicación.

El instrumento tiene que ser abierto y no prohibir un arma o método en específico porque éstos se encuentran en constante evolución.

La declaración deberá referir explícitamente que los principios reguladores del derecho internacional humanitario son: la distinción, la proporcionalidad, la necesidad militar y la humanidad. Consecuentemente, se elaborará lo necesario sobre su contenido.

Como parte de los principios reguladores del derecho internacional humanitario no se contemplará la neutralidad o la caballería, puesto que el propósito de este trabajo es acotar los elementos esenciales que deben ser cubiertos en un instrumento jurídico que dé pie al desarrollo del derecho aplicable a través de la práctica. Consecuentemente, el instrumento que se propone cubrirá únicamente los aspectos que se consideran esenciales en torno a los principios ya referidos.

El instrumento debe contener una provisión que refiera la relevancia del derecho internacional humanitario convencional y consuetudinario existente, así como su desarrollo a través de la jurisprudencia y la doctrina. De esta forma, el instrumento proveerá las herramientas necesarias para que los Estados apliquen el derecho internacional humanitario a la ciberguerra de la mejor manera.

Así, en el siguiente apartado se expondrá la propuesta de resolución de la Asamblea General que adopta la declaración sobre la aplicación del derecho

internacional humanitario a la ciberguerra. El contenido de la propuesta resulta de todo el análisis y conclusiones alcanzadas en este trabajo.

4.4. Propuesta concreta de instrumento jurídico

Declaración sobre la aplicación del derecho internacional humanitario a la guerra cibernética

La Asamblea General,

Recordando los hallazgos del Grupo de Trabajo de Composición Abierta creado por la Asamblea General para abordar el tema “Avances en la Esfera de la Información de las Telecomunicaciones en el Contexto de la Seguridad Internacional” (A/AC.290/2021/CRP.2), en particular que dentro de las amenazas existentes y potenciales a la paz y seguridad internacional se encuentra el hecho de que los Estados desarrollan cada vez más sus capacidades en el campo de las tecnologías de la información y la comunicación con propósitos militares,

Recordando que el Grupo de Expertos Gubernamentales establecido por Naciones Unidas para abordar el tema “Desarrollo en el Campo de las Tecnologías de la Información y la Comunicación en el Contexto de la Seguridad Internacional” (A/70/174) concluyó que los principios de humanidad, necesidad, proporcionalidad y distinción aplican al uso que los Estados dan a las tecnologías de la información y la comunicación,

Aprueba la Declaración sobre la aplicación del derecho internacional humanitario a la guerra cibernética.

Anexo

Declaración sobre la aplicación del derecho internacional humanitario a la guerra cibernética

La Asamblea General,

Observando los progresos constantes y vertiginosos en el desarrollo y la aplicación de nuevas tecnologías en los conflictos armados,

Resaltando la importancia de respetar las normas y principios del derecho internacional humanitario con el propósito de evitar sufrimiento innecesario,

Convencida de la importancia de cumplir con la obligación de realizar el examen legal *ex ante* a nuevos medios o métodos de guerra de conformidad con el artículo 36 del Protocolo Adicional I a los Convenios de Ginebra de 1949, incluidos los medios y métodos de guerra cibernética,

Destacando la relevancia del Comité Internacional de la Cruz Roja como organización que promueve el respeto del derecho internacional humanitario,

Reconociendo la necesidad de alcanzar un entendimiento común sobre la aplicación del derecho internacional humanitario en el ciberespacio,

Destacando que, debido al desarrollo constante de las tecnologías aplicadas a los conflictos armados, se necesitan normas y principios de aplicación amplia que permitan a los Estados un margen de actuación razonable respecto de la aplicación del derecho internacional humanitario en el ciberespacio,

Convencida de que la presente “Declaración sobre la aplicación del derecho internacional humanitario a la guerra cibernética” servirá como base y guía para la aplicación del derecho de la guerra en la conducción de las

hostilidades que usen el ciberespacio, a fin de que tanto los individuos, como las instituciones y los Estados, inspirándose en ella, promuevan el respeto a su contenido y así, a través de la práctica, el derecho internacional humanitario sea aplicado cada vez de forma más clara y constante en la ciberguerra,

Declara lo siguiente:

Artículo 1

Se entiende que:

a. Ciberespacio significa: el entorno formado por componentes físicos y no físicos que permiten el tráfico de información entre dispositivos varios interconectados en distintos niveles de alcance a través de redes informáticas.
b. Red informática significa: un conjunto de dispositivos informáticos autónomos interconectados. Se dice que dos ordenadores están interconectados si pueden intercambiar información. La interconexión puede realizarse a través de diversos medios de transmisión
c. Infraestructura cibernética significa: los dispositivos de comunicación, almacenamiento y computación sobre los que se construyen y funcionan los sistemas de información.
d. Operación cibernética significa: empleo de capacidades del ciberespacio para alcanzar objetivos en o a través de éste. Se dividen en operaciones de ataque a redes informáticas y operaciones de explotación de redes informáticas.
e. Operación de ataque a redes informáticas significa: operación cibernética que pretende causar algún perjuicio a la información que contienen

ordenadores y redes informáticas, o pretenden destruir los ordenadores y redes en sí mismas.

f. Operación de explotación de redes informáticas significa: operación que únicamente afecta el ciberespacio, sin proyectarse al mundo físico, como operaciones de reconocimiento, vigilancia y extracción de datos o información.

g. Ciberguerra o guerra cibernética significa: operaciones lanzadas contra un ordenador o un sistema de ordenadores a través de una corriente de datos, cuando se usan como medios y métodos de guerra en el contexto de un conflicto armado según se encuentra definido en el derecho internacional humanitario.

h. Ataque cibernético significa: cualquier operación cibernética llevada a cabo sin el consentimiento o conocimiento del propietario del sistema objetivo, que se espera razonablemente que cause lesiones o muerte a personas o daños o destrucción de objetos, incluida la pérdida de funcionalidad.

i. Medio de guerra cibernética significa: códigos computacionales que se utilizan, o están diseñados para ser utilizados, con el objetivo de amenazar con o causar daños físicos, funcionales o mentales a estructuras, sistemas o seres vivos. Incluye dispositivos, materiales, instrumentos, mecanismos, equipamiento o programas diseñados para realizar un ataque cibernético.

j. Método de guerra cibernética significa: las tácticas, técnicas y procedimientos cibernéticos por los cuales se conducen las hostilidades.

Se refieren a cómo se llevan a cabo las operaciones cibernéticas, que se distinguen de los instrumentos utilizados para conducirlas.

Artículo 2

2.1. El derecho internacional humanitario regula la conducción de las hostilidades en conflictos armados internacionales y no internacionales, independientemente de los medios o métodos de guerra que se empleen. Esto incluye el desarrollo de los conflictos armados a través de la ciberguerra.

2.2. El derecho internacional humanitario regula las operaciones cibernéticas que se constituyan en ataques cibernéticos, ya sea que deriven de operaciones de ataque a redes informáticas o de éstas en relación con operaciones de explotación de redes informáticas.

Artículo 3

3.1. El derecho internacional humanitario regula el uso de medios y métodos de guerra cibernética, así como los ataques cibernéticos, con base en los principios reguladores del derecho internacional humanitario de carácter consuetudinario: distinción, proporcionalidad, necesidad militar y humanidad.

3.2. En la aplicación de estos principios a la conducción de la ciberguerra, las partes en un conflicto armado deberán tener en cuenta, en primer lugar, su desarrollo en el derecho convencional y consuetudinario, así como, en segundo lugar, su desarrollo jurisprudencial y doctrinario. De tal forma que se favorezca la interpretación más próxima a la esencia de los principios mencionados y la

aplicación más razonable y compatible con las características propias del ciberespacio y la ciberguerra.

Artículo 4

4.1. El principio de distinción implica que las partes en un conflicto armado deben diferenciar en todo momento entre población civil y combatientes, así como entre bienes de carácter civil y objetivos militares.

4.2. Los ataques cibernéticos deben dirigirse únicamente contra combatientes y objetivos militares.

4.3. Los objetivos militares son aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar y cuya destrucción total o parcial, captura o neutralización ofrece, en las circunstancias del caso, una ventaja militar definida.

Artículo 5

5.1. Los objetos de uso dual, como la infraestructura cibernética, únicamente pueden ser atacados si constituyen objetivos militares lícitos.

5.2. En caso de llevar a cabo un ataque cibernético contra un objeto de uso dual, se deberán respetar los principios reguladores del derecho internacional humanitario.

Artículo 6

6.1. Los ataques cibernéticos no deben ser indiscriminados.

6.2. Al realizar ataques cibernéticos, se deben tomar todas las precauciones factibles para evitar o minimizar daños a la población y objetos civiles, ya sea por efectos directos o indirectos.

Artículo 7

7.1. Los ataques cibernéticos solamente deben ser lanzados desde sistemas informáticos operados por combatientes. Por lo que, no deben utilizarse sistemas informáticos distintos como intermediarios para realizar ataques cibernéticos.

7.2. El párrafo anterior es sin perjuicio de que los ataques cibernéticos se beneficien de la infraestructura cibernética de uso dual, tal como medio para el tráfico de datos.

Artículo 8

El principio de proporcionalidad implica que un ataque cibernético está prohibido cuando: sea de prever que causará incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas consecuencias, que serían excesivas en relación con la ventaja militar concreta y directa prevista.

Artículo 9

El principio de necesidad militar implica que una parte en un conflicto armado únicamente puede recurrir a los medios y métodos de guerra cibernética necesarios para alcanzar el propósito de debilitar a las fuerzas militares del enemigo.

Artículo 10

El principio de humanidad implica que se debe limitar el sufrimiento, las lesiones y la destrucción provocada por la guerra cibernética, con el propósito de proteger la vida, la salud y asegurar el respeto por el ser humano.

4.5. Conclusiones

Derivado de lo expuesto en este capítulo, se concluye que:

- Las propuestas existentes sobre la creación de un instrumento jurídico que regule la ciberguerra usualmente tienden a la creación de un tratado internacional.
- Un instrumento jurídico *soft law* es viable como base para el desarrollo de la aplicación del derecho internacional humanitario al ciberespacio.
- Una declaración aprobada por una resolución de la Asamblea General de Naciones Unidas es un medio adecuado para expresar la voluntad de aplicar el derecho internacional humanitario al ciberespacio y establecer sus términos.

Conclusiones generales

PRIMERA. El derecho internacional humanitario regula únicamente la conducción de los conflictos armados, no cómo y cuándo se iniciaron, en tanto que es el *jus in bello*.

SEGUNDA. Las fuentes del derecho internacional humanitario son: tratados, costumbre y principios generales de derecho.

TERCERA. El desarrollo convencional del derecho internacional humanitario se divide, esencialmente, en tres rubros, según el lugar en el que se desarrolló: La Haya, Ginebra y Nueva York.

CUARTA. Desde 2015, la Organización de las Naciones Unidas dedica esfuerzos constantes a dilucidar el derecho aplicable a las tecnologías de la información y la comunicación en el contexto de la paz y seguridad internacional.

QUINTA. El derecho internacional humanitario convencional no regula la conducción de las hostilidades a través del ciberespacio.

SEXTA. Los principios del derecho internacional humanitario emanan tanto de tratados como de la costumbre internacional, al mismo tiempo que constituyen principios generales de derecho.

SÉPTIMA. Los principios fundamentales que regulan el derecho internacional humanitario son: distinción, proporcionalidad, necesidad militar y humanidad.

OCTAVA. Los principios del derecho internacional humanitario expresan la sustancia de este régimen jurídico y sirven de directrices en los casos no previstos. Además, estos principios son de observancia obligatoria para todos los Estados.

NOVENA. Los principios de humanidad, necesidad, proporcionalidad y distinción son aplicables en el uso de las tecnologías de la información y la comunicación.

DÉCIMA. El artículo 36 del “Protocolo Adicional I a los Convenios de Ginebra” de 1949 consagra la obligación de realizar un examen jurídico a los medios y métodos de guerra nuevos, con la finalidad de que su empleo respete los principios y normas del derecho internacional humanitario.

DÉCIMA PRIMERA. El derecho internacional humanitario regula el uso de medios y métodos de guerra. Los primeros se refieren a las armas; mientras que, los segundos se refieren a las formas en que las armas pueden ser usadas o la manera en que las hostilidades pueden ser conducidas.

DÉCIMA SEGUNDA. El ciberespacio es el entorno formado por componentes físicos y no físicos que permiten el tráfico de información entre dispositivos varios interconectados en distintos niveles de alcance a través de redes informáticas.

DÉCIMA TERCERA. Las operaciones cibernéticas implican el empleo de capacidades del ciberespacio para alcanzar objetivos en o a través de éste.

DÉCIMA CUARTA. En general, las operaciones cibernéticas quedan comprendidas en el modelo *kill chain model*: 1) se realiza el reconocimiento del objetivo, 2) se prepara el programa que se utilizará para realizar la operación, 3) se transmite el programa maligno, 4) se activa el programa que aprovechará las debilidades y fallas del objetivo, 5) el programa instala un acceso permanente para permitir que el dispositivo o sistema objetivo sea manipulado externamente, 6) se toma control del dispositivo o sistema antes mencionado, y 7) se realizan las acciones pretendidas para alcanzar el propósito de la operación.

DÉCIMA QUINTA. Las operaciones cibernéticas se dividen en dos tipos, según sus efectos: operaciones de ataque a redes informáticas y operaciones de explotación de redes informáticas.

DÉCIMA SEXTA. Las operaciones de ataque a redes informáticas pretenden causar algún perjuicio a la información que contienen ordenadores y redes informáticas, o pretenden destruir los ordenadores y redes en sí mismas.

DÉCIMA SÉPTIMA. Las operaciones de explotación de redes informáticas únicamente afectan el ciberespacio, sin proyectarse al mundo físico, como operaciones de reconocimiento, vigilancia y extracción de datos o información

DÉCIMA OCTAVA. La guerra cibernética o ciberguerra se constituye por las operaciones lanzadas contra un ordenador o un sistema de ordenadores a través de una corriente de datos, cuando se usan como medios y métodos de guerra en el contexto de un conflicto armado según se encuentra definido en el derecho internacional humanitario.

DÉCIMA NOVENA. El uso de operaciones cibernéticas en la conducción de las hostilidades está presente hoy día, lo que evidencia la necesidad de abordar los principios reguladores del derecho internacional humanitario que aplican en tales casos.

VIGÉSIMA. El derecho internacional humanitario regula los medios y métodos de guerra cibernética, así como los ataques cibernéticos.

VIGÉSIMA PRIMERA. Un ataque cibernético es cualquier operación cibernética llevada a cabo sin el consentimiento o conocimiento del propietario del sistema objetivo, que se espera razonablemente que cause lesiones o muerte a personas o daños o destrucción de objetos, incluida la pérdida de funcionalidad.

VIGÉSIMA SEGUNDA. Un medio de guerra cibernética se compone de códigos computacionales que se utilizan, o están diseñados para ser utilizados, con el objetivo de amenazar con o causar daños físicos, funcionales o mentales a estructuras, sistemas o seres vivos. Incluye dispositivos, materiales, instrumentos, mecanismos, equipamiento o programas diseñados para realizar un ataque cibernético.

VIGÉSIMA TERCERA. Un método de guerra cibernética se compone de las tácticas, técnicas y procedimientos cibernéticos por los cuales se conducen las hostilidades. Se refieren a cómo se llevan a cabo las operaciones cibernéticas, que se distinguen de los instrumentos utilizados para conducirlas.

VIGÉSIMA CUARTA. El artículo 36 del "Protocolo Adicional I a los Convenios de Ginebra" de 1949 implica un mecanismo de revisión *ex ante* sobre la licitud del empleo de medios o métodos de guerra cibernética en el contexto de un conflicto armado, el cual exige asegurar la legalidad del empleo del medio o método en cuestión desde su etapa más temprana de desarrollo.

VIGÉSIMA QUINTA. La revisión legal que se consagra en el artículo 36 del "Protocolo Adicional I a los Convenios de Ginebra" de 1949 deben realizarla incluso los Estados no parte del Protocolo Adicional, pues de lo contrario se arriesgan a violar las normas y principios consuetudinarios del derecho internacional humanitario.

VIGÉSIMA SEXTA. Los principios reguladores del derecho internacional humanitario, es decir, distinción, proporcionalidad, necesidad militar y humanidad, regulan los medios y métodos de guerra cibernética, así como cualquier operación cibernética que se configure como un ataque cibernético.

VIGÉSIMA SÉPTIMA. El instrumento jurídico que regule la ciberguerra debe contener términos amplios y ser flexible en función de ir a la par del desarrollo tecnológico y permitir que los Estados desarrollen la práctica estatal pertinente.

VIGÉSIMA OCTAVA. Hasta ahora, las propuestas sobre la regulación de la ciberguerra han planteado la creación de un tratado internacional.

VIGÉSIMA NOVENA. No hay propuestas que consideren la regulación de la ciberguerra a través de un instrumento *soft law* como una declaración o una resolución de la Asamblea General de Naciones Unidas.

TRIGÉSIMA. Suele ser más sencillo concluir un instrumento *soft law* que un tratado, el cual habitualmente se considera *hard law*.

TRIGÉSIMA PRIMERA. Los instrumentos jurídicos *soft law* han servido y sirven de base para el desarrollo progresivo del derecho internacional en distintos ámbitos.

TRIGÉSIMA SEGUNDA. Los instrumentos legales del tipo *soft law* son ideales para guiar el actuar de los Estados y permitir que desarrollen la práctica estatal pertinente de forma paulatina.

TRIGÉSIMA TERCERA. Empecinarse en crear un tratado para regular la ciberguerra podría retrasar la adopción de un instrumento jurídico que la regule. En cambio, la creación de un instrumento *soft law* permitiría tener una base escrita y consensuada para desarrollar el derecho internacional humanitario aplicable a la guerra cibernética.

TRIGÉSIMA CUARTA. La declaración que se plantea en esta tesis sobre la aplicación del derecho internacional humanitario a la guerra cibernética es apropiada para guiar la práctica estatal.

TRIGÉSIMA QUINTA. Que la Asamblea General de Naciones Unidas adopte la declaración que se propone en esta tesis ayudaría a conjuntar el consenso estatal sobre su contenido y motivaría la voluntad para su cumplimiento.

Referencias

Bibliografía

ANDRESS, J. y WINTERFELD, S., Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 2a ed., Syngress, Estados Unidos, 2014.

APPLEGATE, Scott, “The Dawn of Kinetic Cyber”, en PODINS, K., STINISSEN, J. y MAYBAUM, M.(eds.), 5th International Conference on Cyber Conflict, S.N.E., Tallin, 2013.

BIGSON, William, “Neuromancer”, citado por DELERUE, François, Cyber Operations and International Law, S.N.E., Cambridge University Press, Reino Unido, 2020.

BOULANIN, Vincent y VERBRUGGEN, Maaike, Article 36 reviews: dealing with the challenges posed by emerging technologies, S.N.E., SIPRI, Suecia, 2017.

BRANGETTO, Pascal, ÇALIŞKAN, Emin y RÕIGAS, Henry, Cyber Red Teaming: Organisational, technical and legal implications in a military context, S.N.E., CCDCOE, Tallin, 2015.

CHAYES, A., Borderless Wars: Civil Military Disorder and Legal Uncertainty, S.N.E., Cambridge University Press, Estados Unidos, 2015.

CLARKE, Richard y KNAKE, Robert, “Cyber War: The Next Threat to National Security and What to Do About It”, citado por VALERIANO, Brandon y MANESS, Ryan, Cyber War versus Cyber Realities: cyber conflict in the international system, S.N.E., Oxford University Press, Nueva York, 2015.

CRWE, Jonathan y WESTON-SCHEUBER, Kylie, Principles of International Humanitarian Law, S.N.E., Edward Elgar Publishing Limited, Cheltenham, 2013.

CUNNINGHAM, Chase, Cyber Warfare – Truth, Tactics, and Strategies, S.N.E., Packt Publishing, Reino Unido, 2020.

DALZIEL, H., Securing Social Media in the Enterprise, S.N.E., Syngress, Estados Unidos, 2015.

DELERUE, François, Cyber Operations and International Law, S.N.E., Cambridge University Press, Reino Unido, 2020.

DINSTEIN, Yoram, The Conduct of Hostilities under the Law of International Armed Conflict, S.N.E., Cambridge University Press, Nueva York, 2004.

GISEL, Laurent y OLEJNIK, Lukasz, The potential human cost of cyber operations, S.N.E., ICRC, Ginebra, 2019.

GISEL, Laurent, The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law, S.N.E., ICRC, Canadá, 2016.

GUTIÉRREZ BAYLÓN, Juan de Dios, Sistema jurídico de las Naciones Unidas, S.N.E., Editorial Porrúa, México, D.F., 2007

HARRISON DINNISS, Heather, Cyber Warfare and the Laws of War, S.N.E., Cambridge University Press, Reino Unido, 2012.

HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume I: Rules, S.N.E., Cambridge University Press, Cambridge, 2005.

HENCKAERTS, Jean-Marie y DOSWALD-BECK (eds.), Louise, Customary International Humanitarian Law Volume II: Practice – Part 1 and Part 2, S.N.E., Cambridge University Press, Cambridge, 2005.

HILDRETH, Steven A., CRS Report for Congress Cyberwarfare, The Library of Congress, 2001.

KALSHOVEN, Frits y ZEGVELD, Liesbeth, Restricciones en la conducción de la guerra: introducción al derecho internacional humanitario, 2ª ed., Comité Internacional de la Cruz Roja, trad. Margarita Polo, Buenos Aires, 2005.

KALSHOVEN, Frits, "*Reaffirmation and development of international humanitarian law applicable in armed conflicts: the conference of government experts (second session)*", en International Review of the Red Cross, Ginebra, junio-julio 1971.

KOLB, Robert, Advanced Introduction to International Humanitarian Law, S.N.E., Edward Elgar Publishing Limited, Reino Unido, Cheltenham, 2014.

LAWAND, K., Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos: medidas para aplicar el artículo 36 del Protocolo Adicional I de 1977, S.N.E., Comité Internacional de la Cruz Roja, Ginebra, 2006.

LIBICKI, Martin, Cyberdeterrence and Cyberwar, S.N.E., RAND Corporation, Estados Unidos, 2009.

LIVOJA, Rain y McCORMACK, Tim (eds.), Routledge Handbook of the Law of Armed Conflict, S.N.E., Routledge, New York, 2016.

MARYLISE, Nellly, Storm Worm: A P2P Botnet, S.N.E., Norwegian University of Science and Technology, Noruega, 2008.

MELZER, Nils, International Humanitarian Law: A Comprehensive Introduction, S.N.E., International Committee of the Red Cross, Suiza, Ginebra, 2019.

NYE, Joseph, “The Future of Power”, citado por VALERIANO, Brandon y MANESS, Ryan, Cyber War versus Cyber Realities: cyber conflict in the international system, S.N.E., Oxford University Press, Nueva York, 2015.

OFFICE OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF, DOD Dictionary of Military and Associated Terms, S.N.E., Washington DC, 2021.

PICTET, Jean S., Commentary on the Geneva Conventions of 12 August 1949 relative to the Treatment of Prisoners of War, S.N.E., ICRC, trad. A. P. de Heney, Geneva, 1960.

PICTET, Jean, “Développement et príncipes du droit international humanitaire”, citado por SALMÓN, Elizabeth, Introducción al Derecho Internacional Humanitario, 3ª ed., Comité Internacional de la Cruz Roja, Perú, Lima, 2012.

RID, Thomas y McBURNEY, Peter, “Cyber Weapons”, citado por VALERIANO, Brandon y MANESS, Ryan, Cyber War versus Cyber Realities, 2015.

ROSCINI, Marco, Cyber Operations and the Use of Force in International Law, S.N.E., Oxford University Press, Reino Unido, 2014.

SALMÓN, Elizabeth, Introducción al Derecho Internacional Humanitario, 3ª ed., Comité Internacional de la Cruz Roja, Perú, Lima, 2012.

SANDOZ, Yves, *et al.* (eds.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, S.N.E., Martinus Nijhoff Publishers, Ginebra, 1987.

SAUL, Ben y AKANDE, Dapo (eds.), The Oxford Guide to International Humanitarian Law, S.N.E., Oxford University Press, New York, 2020.

SCHMITT, Michael N., Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, 2a ed., Cambridge University Press, Reino Unido, 2017.

SHACKELFORD, S., Douzet, F. y ANKERSEN, C. (eds.), Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace, S.N.E., Cambridge University Press, Estados Unidos, 2022.

SHAFFER, G. y POLLAK, M., "*Hard and Soft Law"*, en DUNOFF, J. y POLLAK, M. (eds.), Interdisciplinary Perspectives on International Law and International Relations: The State of the Art, S.N.E., Cambridge University Press, Reino Unido, 2012.

SIMON, T. y la Comisión Global sobre Gobernanza de Internet, "*Critical infrastructure and the internet of things*", en Cyber Security in a Volatile World, S.N.E., 2017.

SPRINGER, Paul J., Cyber Warfare, S.N.E., ABC-CLIO, Reino Unido, 2015.

TANENBAUM, Andrew, FEAMSTER, Nick y WETHERALL, David, Computer Networks, 6a ed., Pearson Education Limited, Reino Unido, 2021.

Hemerografía

ATREWS, R., "*Cyberwarfare*", en Journal of Information Warfare, Peregrine Technical Solutions, Estados Unidos, Vol. 19, Núm. 4, 2020.

BARTELS, Rogier, "*Timelines, borderlines and conflicts: The historical evolution of the legal divide between international and non-international armed conflicts*", en International Review of the Red Cross, ICRC, Geneva, 2009, Vol. 91, Núm. 873, marzo 2009.

BERGH, A., "*Understanding Influence Operations in Social Media: A cyber Kill Chain Approach*", en Journal of Information Warfare, Vol. 19(4), 2020.

BOOTHBY, W., "*Methods and Means of Cyber Warfare*", en International Law Studies, U.S. Naval War College, Estados Unidos, Vol. 89, 2013.

BOTHE, Michael, "*Legal and Non-Legal Norms - a meaningful distinction in international relations?*", en Netherlands Yearbook of International Law, Vol. 11, 1980.

BOYLE, Alan, "*Some Reflections on the Relationship of Treaties and Soft Law*", en The International and Comparative Law Quarterly, Vol. 48, Núm. 4, 1999, págs. 901-902.

BRANTLY, A., "*The Violence of Hacking: State Violence and Cyberspace*", en The Cyber Defence Review, Army Cyber Institute, Estados Unidos, Vol. 2, Núm. 1, 2017.

BROWN, D. "*A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*", en Harvard International Law Journal, Vól. 47, Núm. 1, 2006.

EASTTOM, C., "*An Examination of the Operational Requirements of Weaponised Malware*", en Journal of Information Warfare, Peregrine Technical Solutions, Estados Unidos, Vol. 17, Núm. 2, 2018.

EFRONY, Dan y SHANY, Yuval, "*A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*", en The American Journal of International Law, Cambridge University Press, Estados Unidos, Vol. 112, Vol. 4, 2018.

FRANKLIN, A., "*An International Cyber Warfare Treaty Historical Analogies and Future Prospects*", en Journal of Law & Cyber Warfare, Vol. 7, Núm. 1, 2018.

GEISS, R. y LAHMANN, H., "*Cyber warfare: applying the principle of distinction in an interconnected space*", en Israel Law Review, Cambridge University Press, Reino Unido, Vol. 45, Núm. 3, 2012.

GUNNERIUSSON, H. y OTTIS, R, "*Cyberspace from the Hybrid Threat Perspective*", en Journal of Information Warfare, Peregrine Technical Solutions, Estados Unidos, Vol.12, Núm. 3, 2013.

HAATAJA Samuli y AKHTAR-KHAVARI, Afshin, "*Stuxnet and International Law on the Use of Force: an International Approach*", en Cambridge International Law Journal, Vol.7, 2018.

HARKINS, M. y FREED, A., "*The Ransomware Assault on the Healthcare Sector*", en Journal of Law & Cyber Warfare, Lexeprint, Inc, Estados Unidos, Vol. 6(2), 2018.

HATHAWAY, Oona, *et al.*, "*The Law of Cyber-Attack*", en California Law Review, California Law Review Inc., Estados Unidos, Vol. 100, Núm. 4, 2012.

HOLZ, Thorsten, *et al.*, "*Measures and Mitigation of Peer-to-Peer-based Botnets: A case Study on Storm Worm*", en Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Trheats, Estados Unidos, Núm. 9, 2008.

HUGHES, R., "*A treaty for cyberspace*", en International Affairs (Royal Institute of International Affairs 1944-), Vol. 86, 2010.

JACOBSSON, Marie y MARJA, Lehto, "*Protection of the Environment in Relation to Armed Conflicts – An Overview of the International Law Commission's*

Ongoing Work", en Goettingen Journal of International Law, Alemania, 2020, Vol.10, Núm. 1,17 de julio del 2020.

JEVGLEVSKAJA, N., "*Legal Review of New Weapons: Origins of Article 36 of AP I*", en Finnish Yearbook of International Law, Finlandia, Vol. 25, 2017.

KELSEY, Jeffrey, "*Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*", en Michigan Law Review, The Michigan Law Review Association, Estados Unidos, 2008, Vol.106, Núm. 7.

KHAN, R, *et al.*, "*Threat Analysis of BlackEnergy for Synchrophasor based Real-timeControl and Monitoring in Smart Grid*", en 4th International Symposium for ICS & SCADA Cyber Security Research, 23-25 agosto de 2016.

MALIARCHUK, Tamara, "*Hybrid Warfare and Cyber Effects in Energy Infrastructure*", en *Connections*, Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Alemania, Vol.18, Núm. 1, 2019.

McCLELLAND, J., "*The Review of weapons in accordance with Article 36 of Additional Protocol I*", en International Review of the Red Cross, Ginebra, Vol. 85, Núm. 850, 2003.

McFARLAND, T. y ASSAAD, Z., "*Legal Reviews of* in situ *learning in autonomous weapons*", en Ethics and Information Technology, Vol. 25, Núm. 9, 2023.

MELE, S., "*Legal Considerations on Cyber-Weapons and Their Definition*", en Journal of Law & Cyber Warfare, Lexeprint, Vol. 3, Núm. 1, 2014.

MILANOVIC, M. y SCHMITT, M., "*Cyber Attacks and Cyber (Mis) information Operations During a Pandemic*", en Journal of National Security and Law & Policy, Estados Unidos, Vol. 11, 2020.

MOHURLE, S. y PATIL, M., "*A brief study of Wannacry Threat: Ransomware Attack 2017*", en International Journal of Advanced Research in Computer Science, Vol. 8, Núm. 5, 2017.

OLIVIER, Michele, "*The relevance of 'soft law' as a source of international human rights*", en The Comparative and International Law Journal of Southern Africa, Vol. 35, Núm. 3, 2002.

POOL, Phillip, "*War of the Cyber World: The Law of Cyer Warfare*", en The International Lawyer, American Bar Association, Estados Unidos, Vol. 47, Núm. 2, 2013.

ROSANA, C., "*A Game of Code: Challenges of Cyberspace as a Domain of Warfare*", en Strathmore Law Review, Vol. 3, 2018.

ROSANA, C., "*A Game of Code: Challenges of Cyberspace as a Domain of Warfare*", en Strathmore Law Review, Vol. 3, 2018.

TALBOT, Eric, "*Cyber Warfare and Precautions against the Effects of Attacks*", en Texas Law Review, Vol. 88, 2009.

TALBOT, Eric, "*Cyber Warfare and Precautions against the Effects of Attacks*", en Texas Law Review, Vol. 88, 2009.

VITÉ, Silvain, "*Typology of armed conflicts in international humanitarian law: legal concepts and actual situations, International Review of the Red Cross*", en International Review of the Red Cross, Geneva, Vol. 91, Núm. 873, marzo 2009.

Tratados

“Carta de las Naciones Unidas”, San Francisco, Estados Unidos de América, 25 de junio de 1945, D.O.F. 17 de octubre de 1945.

“Convención de 2008 sobre Municiones de Racimo”, Dublín, Irlanda, 30 de mayo de 2008, D.O.F. 30 de julio de 2010.

“Convención para la protección de los bienes culturales en caso de conflicto armado”, La Haya, Holanda, 14 de mayo de 1954, D.O.F. 3 de agosto de 1956.

“Convención relativa a ciertas restricciones en cuanto al ejercicio de derecho de captura en la guerra marítima (H.XI)”, La Haya, Holanda, 18 de octubre de 1907, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1907-conv-restrictions-capture-naval-war-5tdm2t.htm.

“Convención relativa a la colocación de minas submarinas automáticas de contacto (H.VIII)”, La Haya, Holanda, 18 de octubre de 1907, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1907-conv-submarine-contact-mines-5tdm35.htm#:~:text=Es%20prohibido%20colocar%20minas%20autom%C3%A1ticas,seguridad%20de%20la%20navegaci%C3%B3n%20pac%C3%ADfica.

“Convención relativa a las leyes y costumbres de la guerra terrestre”, La Haya, Holanda, 18 de octubre de 1907,

https://www.icrc.org/es/doc/resources/documents/misc/treaty-1907-hague-convention-4-5tdm34.htm.

“Convención sobre la prohibición de utilizar técnicas de modificación ambiental con fines militares u otros fines hostiles”, Nueva York, Estados Unidos, 10 de diciembre de 1976, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1976-enmod-convention-5tdm2l.htm.

“Convención sobre la prohibición del desarrollo, la producción y el almacenamiento de armas bacteriológicas (biológicas) y toxínicas y sobre su destrucción’’, Londres, Moscú y Washington, 10 de abril de 1972, D.O.F. 12 de agosto de 1974.

“Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas y sobre su destrucción”, Ginebra, Suiza, 3 de septiembre de 1992, D.O.F. 5 de octubre de 1994.

“Convención sobre la prohibición del empleo, almacenamiento, producción y transferencia de minas antipersonal y sobre su destrucción”, Oslo, Noruega 18 de septiembre de 1997, D.O.F. 21 de agosto de 1998.

“Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados”, 10 de octubre de 1980, D.O.F. 4 de mayo de 1982.

“Convenio de Ginebra del 22 de agosto de 1864 para el mejoramiento de la suerte de los militares heridos en los ejércitos en campaña”, Ginebra, Holanda, 22 de agosto de 1864, https://www.icrc.org/es/doc/resources/documents/treaty/treaty-1864-

geneva-convention-1.htm#:~:text=En%201864%2C%20el%20Consejo%20Federal,agosto%20del%20mismo%20a%C3%B1o%20y.

"Convention (IX) concerning Bombardment by Naval Forces in Time of War", La Haya, Holanda, 18 de octubre de 1907, https://ihl-databases.icrc.org/assets/treaties/220-IHL-24-EN.pdf.

"Convention (X) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention", La Haya, Holanda, 18 de octubre de 1907, https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-x-1907?activeTab=historical.

"Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field. Geneva, 27 July 1929", Ginebra, Suiza, 27 de julio de 1929, https://ihl-databases.icrc.org/es/ihl-treaties/gc-wounded-1929?activeTab=historical.

"El Convenio de Ginebra del 27 de julio de 1929 relativo al trato debido a los prisioneros de guerra", Ginebra, Suiza, 27 de julio de 1929, https://www.icrc.org/es/doc/resources/documents/misc/5tdmyg.htm#:~:text=En%20%C3%A9l%20se%20plantea%20el,ejercer%20represalias%20en%20su%20contra.

"III. Convenio de Ginebra relativo al trato debido a los prisioneros de guerra", Ginebra, Suiza, 8 de diciembre de 1949, D.O.F. 23 de junio de 1953.

"IV. Convenio de Ginebra relativo a la protección debida a las personas civiles en tiempo de guerra", Ginebra, Suiza, 8 de diciembre de 1949, D.O.F. 23 de junio de 1953.

“Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I)”, Ginebra, Suiza, 12 de agosto de 1949, D.O.F. 21 de abril de 1983.

“Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la aprobación de un signo distintivo adicional (Protocolo III)”, Ginebra, Suiza, 8 de diciembre de 2005, D.O.F. 5 de enero de 2009.

“Protocolo II adicional a los Convenios de Ginebra del 12 de agosto 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional”, Ginebra, Suiza, 8 de junio de 1977, https://www.icrc.org/es/doc/resources/documents/misc/protocolo-ii.htm.

“Protocolo para la protección de los bienes culturales en caso de conflicto armado”, La Haya, Holanda, 14 de mayo de 1954, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1954-hague-convention-protocol-1-5tdm38.htm.

“Protocolo sobre Armas Láser Cegadoras (Protocolo IV)”, Ginebra, Suiza, 8 de octubre de 1995, D.O.F. 27 de mayo de 1998.

“Protocolo sobre fragmentos no localizables (Protocolo I)”, Ginebra, Suiza, 10 de octubre de 1980, D.O.F. 4 de mayo de 1982.

“Protocolo sobre la prohibición del uso en la guerra, de gases asfixiantes, tóxicos o similares y de medios bacteriológicos”, Ginebra, Suiza, 17 de junio de 1925, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1925-gases-and-bacteriological-protocol-5tdm2p.htm.

“Protocolo sobre los Restos Explosivos de Guerra (Protocolo V)”, Ginebra, Suiza, 28 de noviembre 2003, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1980-cccw-protocol-5-erw-5x6lck.htm.

“Protocolo sobre prohibiciones o restricciones del empleo de armas incendiarias (Protocolo III)”, Ginebra, Suiza, 10 de octubre de 1980, D.O.F. 4 de mayo de 1982.

“Protocolo sobre Prohibiciones o Restricciones del Empleo de Minas, Armas Trampa y Otros Artefactos (Protocolo II)”, Ginebra, Suiza, 10 de octubre de 1980, D.O.F. 4 de mayo de 1982.

“Reglamento relativo a las leyes y costumbres de la guerra terrestre'', La Haya, Holanda, 18 de octubre de 1907, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1907-regulations-laws-customs-war-on-land-5tdm39.htm.

“Reglas de la guerra aérea”, La Haya, Holanda, 28 de febrero de 1923, https://www.icrc.org/es/doc/resources/documents/misc/treaty-1923-rules-air-warfare-5tdm2a.htm#:~:text=Est%C3%A1%20prohibido%20el%20bombardeo%20a%C3%A9reo,pago%20de%20contribuciones%20en%20dinero.

“Segundo Protocolo de la Convención de La Haya de 1954 para la Protección de los Bienes Culturales en caso de Conflicto Armado”, La Haya, Holanda, 26 de marzo de 1999, D.O.F. 14 de abril de 1999.

Documentos de organizaciones internacionales e intergubernamentales

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Advancing responsible State behaviour in cyberspace in the context of international security”, Resolución 73/266, Septuagésimo tercer período de sesiones, 22 de diciembre de 2018.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Compilación de las decisiones de cortes, tribunales y otros órganos internacionales”, Documento de Naciones Unidas A/77/74, Septuagésimo séptimo período de sesiones, 29 de abril de 2022.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Compilación de las decisiones de cortes, tribunales y otros órganos internacionales”, Documento de Naciones Unidas A/74/83, Septuagésimo cuarto período de sesiones, 23 de abril de 2019.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Declaración sobre la concesión de la independencia a los países y pueblos coloniales”, Resolución 1514 (XV), Décimo quinto período de sesiones, 14 de diciembre de 1960.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Declaración Universal de Derechos Humanos”, Resolución 217 A (III), Centésimo octogésimo tercera sesión plenaria, 10 de diciembre de 1948.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Declaration on the prohibition of the use of nuclear and thermo-nuclear weapons”, Resolución 1653 (XVI), Décimo sexto período de sesiones, 24 de noviembre de 1961.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Definición de la agresión”, Resolución 3314 (XXIX), Vigésimo noveno período de sesiones, 14 de diciembre de 1974.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Developments in the field of information and telecommunications in the context of international security”, Resolución 73/27, Septuagésimo tercer período de sesiones, 5 de diciembre de 2018.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Establishment of a nuclear-weapon-free zone in the region of the Middle East”, Resolución 31/71, Trigésimo primer período de sesiones, 10 de diciembre de 1976.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Open-ended working group on developments in the field of information and telecommunications in the context of international security”, Documento de Naciones Unidas A/AC.290/2021/CRP.2, Documento de la sala de conferencias del 10 de marzo de 2021.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, Documento de Naciones Unidas A/70/174, Septuagésimo período de sesiones, 22 de julio de 2015.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security”, Documento de

Naciones Unidas A/76/135, Septuagésimo sexto período de sesiones, 14 de julio de 2021.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Respect for human rights in armed conflicts”, Resolución 2444 (XXIII), Vigésimo tercer período de sesiones, 19 de diciembre de 1968.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, “Responsabilidad del Estado por hechos internacionalmente ilícitos”, Resolución 56/83, Quincuagésimo sexto período de sesiones, 28 de enero de 2002.

COMISIÓN DE DERECHO INTERNACIONAL, “Informe de la Comisión de Derecho Internacional”, Documento de Naciones Unidas A/77/10, 18 de abril a 3 de junio y 4 de julio a 5 de agosto de 2022.

COMISIÓN DE DERECHO INTERNACIONAL, “Report of the International Law Commission to the Sixty-Third Session, Annex E. Protection of the Environment in Relation to Armed Conflicts”, Documento de Naciones Unidas A/66/10, 26 de abril-3 de junio y 4 de julio-12 de agosto de 2011.

COMITÉ DE ASESORES JURÍDICOS SOBRE DERECHO INTERNACIONAL PÚBLICO, Expert Workshop on “Non-Legally Binding Agreements in International Law”, Conferencia en línea, 26 de marzo de 2021.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA, “El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos”, Documento 32IC/15/11, Ginebra, Suiza, 8-10 de diciembre de 2015.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA, “*International humanitarian law and cyber operations during armed conflicts: ICRC position paper*”, Ginebra, Suiza, noviembre, 2019.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA, “The United Nations and International Humanitarian Law: The International Committee of the Red Cross and the United Nations’ involvement in the implementation of international humanitarian law”, en International Committee of the Red Cross, Ginebra, Suiza, 19 de octubre de 1995, [en línea] https://www.icrc.org/en/doc/resources/documents/misc/57jmuk.htm.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA, 26th International Conference of the Red Cross and Red Crescent – Resolutions (and annexes), International Review of the Red Cross, ICRC, Ginebra, 1995, No. 310, Enero-Febrero 1996.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA, Guidelines on the protection of the natural environment in armed conflict: rules and recommendations relating to the protection of the natural environment under international humanitarian law, with commentary, ICRC, Ginebra, 2020.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA, How is the Term “Armed Conflict” Defined in International Humanitarian Law?, Opinion Paper, Geneva, marzo 2008.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Ginebra, 2019.

COMITÉ JURÍDICO INTERAMERICANO, “Directrices del Comité Jurídico Interamericano para los Acuerdos Vinculantes y no Vinculantes”, Washington DC, 1 de noviembre de 2020.

CONSEJO DE LA UNIÓN EUROPEA, “Draft Council conclusions on the Commission and the High Representative of the European Union for Foreign

Affairs and Security Policy joint communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Bruselas, 21 de junio de 2013,.

DEPARTAMENTO DE SERVICIOS DE CONFERENCIAS, "United Nations Editorial Manual", Documento de Naciones Unidas ST/DCS/2, Estados Unidos, 1983.

INSTITUTO EUROPEO DE POLÍTICA ESPACIAL, "ESPI Short Report 1- The war in Ukraine from a space cybersecurity perspective", Austria, octubre de 2022.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, COMISIÓN DE DERECHO INTERNACIONAL, "State responsibility", en Analytical Guide to the Work of the International Law Commission, Ginebra, 2023, [en línea] https://legal.un.org/ilc/guide/9_6.shtml.

PRIMERA COMISIÓN DE NACIONES UNIDAS SOBRE DESARME Y SEGURIDAD INTERNACIONAL, "Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy", Resolución 1(I), Décimo primera sesión plenaria, 24 de enero de 1946.

Decisiones judiciales internacionales

CORTE INTERNACIONAL DE JUSTICIA, Legal Consequences of the Separation of the Chagos Archipielago from Mauritius in 1965. Opinión Consultiva de 25 de febrero de 2019. I.C.J. Reports 2019.

CORTE INTERNACIONAL DE JUSTICIA, Legality of The Threat or Use of Nuclear Weapons. Opinión Consultiva de 8 de julio de 1996. I.C.J. Reports 1996.

CORTE INTERNACIONAL DE JUSTICIA, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Estados Unidos de América). Sentencia de juicio de 27 de junio de 1986. I.C.J. Reports 1986.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, Prosecutor vs. Dragoljub Kunarac, Radomir Kovac y Zoran Vukovic. Sentencia de fondo de 12 de junio de 2002. Caso No. IT-96-23 & IT-96-23/1-A.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, Prosecutor vs. Stanislav Galic. Sentencia de fondo y opinión de 5 de diciembre de 2003. Caso No. IT-98-29-T.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Ramush Haradinaj, Idriz Balaj, and Lahi Brahimaj. Sentencia de fondo de 3 de abril de 2008. Caso No. IT-04-84-T.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Dario Kordic and Mario Cerkez. Sentencia de fondo de 17 de diciembre de 2004. Caso No. IT-95-14/2-A.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Fatmir Limaj, Haradin Bala, and Isak Musliu. Sentencia de fondo de 30 de noviembre de 2005. Caso No. IT-03-66-T.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Naser Oric. Sentencia de fondo de 30 de junio de 2006. Caso No. IT-03-68-T.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Dusko Tadic. Decisión sobre la moción de la defensa para la apelación interlocutoria sobre jurisdicción de 2 de octubre de 1995. Caso No. IT-94-1-A.

TRIBUNAL PENAL INTERNACIONAL PARA LA ANTIGUA YUGOSLAVIA, The Prosecutor vs. Ljube Koskoski Johan Tarculovski. Sentencia de fondo de 10 de julio de 2008. Caso No. IT-04-82-T.

Otras

MACÁK, Kubo y RODENHÄUSER, Tilman, “Cyber operations during armed conflict: the principle of distinction”, en Comité Internacional de la Cruz Roja, Ginebra, Suiza, 7 de marzo de 2023, [en línea] https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf

MACÁK, Kubo y RODENHÄUSER, Tilman, “Cyber operations during armed conflict: the principle of proportionality”, en Comité Internacional de la Cruz Roja, Ginebra, Suiza, 7 de marzo de 2023, [en línea] https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/04_proportionality-0.pdf

MACÁK, Kubo y RODENHÄUSER, Tilman, “Cyber operations during armed conflict: the principles of humanity and necessity”, en Comité Internacional de la Cruz Roja, Ginebra, Suiza, 7 de marzo de 2023, [en línea] https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf

MOORE, David, *et al*, “The Spread of the Sapphire/Slammer Worm”, en Center for Applied Internet Data Analysis, 2003, [en línea] https://www.caida.org/catalog/papers/2003_sapphire/#:~:text=The%20Sapphire%20Worm%20was%20the,UTC%20on%20Saturday%2C%20January%2025.

MUELLER, B., “The laws of war and cyberspace on the need for a treaty concerning cyber conflict”, en LSE IDEAS, 2014, [en línea] https://www.jstor.org/stable/resrep45315.

SECURITY AGENCY, “New Sandworm malware Cyclops Blink replaces VPNFilter, Versión 1.0”, Reino Unido, 23 de febrero de 2022, [en línea] https://www.ncsc.gov.uk/news/new-sandworm-malware-cyclops-blink-replaces-vpnfilter

ZIMMERMANN, Andreas, “The practice of States and International Organisations regarding non-legally binding agreements”, informe para el Comité de Asesores Jurídicos sobre Derecho Internacional Público (CAHDI), Estrasburgo, Francia, 23 de marzo de 2023.