CIBERGUERRA Y DERECHO INTERNACIONAL HUMANITARIO

CT Aud EMILIANO ZITO; CT Aud ANDRÉS ALFREDO PICOLINI; TP Aud LEOPOLDO JUAN FUCELLO; DR. LUIS ALBERTO DEVOTO

RESUMEN

En el presente artículo se analizará la relación que existe en la actualidad entre el Derecho Internacional Humanitario y la Ciberguerra, que se desarrolla en un nuevo teatro de operaciones, el ciberespacio, el cual se caracteriza por su abstracción, así resulta necesario determinar para los conflictos contemporáneos si los principios del Derecho Internacional Humanitario resultan aplicables a este nuevo escenario.

PALABRAS CLAVES

Derecho Militar, Derecho, Ciberguerra, Ciberdefensa, Derecho Internacional, Derecho Internacional Humanitario.

INTRODUCCIÓN

En épocas pasadas, las relaciones del uso de la fuerza por parte de las naciones estaba basada en la doctrina clásica del Derecho de Gentes, los Estados soberanos disponían de plena libertad para hacer uso o no de la fuerza en sus relaciones interestatales. La libre elección del empleo de la fuerza, significaba o representaba la característica más importante de la soberanía en las relaciones internacionales. Por ello, desde los orígenes del Derecho Internacional se vislumbraba la necesidad de someter o subordinar la acción bélica a algún tipo de normativa con la finalidad que el empleo de la fuerza sea compatible con las normas básicas de convivencia internacional y mantenerla dentro de límites o cánones razonables.

Los padres del Derecho Internacional, como Hugo Grocio, Francisco de Vitori y Albérico Gentile; consideraron que las normas de las relaciones internacionales debían organizarse alrededor del problema central de cómo legalizar la guerra. El nacimiento del Derecho Internacional como disciplina separada y distinta de las demás ciencias jurídicas, se debió primordialmente al debate sobre la Guerra Justa y aquella que no lo era, basándose en consideraciones filosóficas e ideológicas. Se considera al año 1864 como al que corresponde a la creación del primer instrumento multilateral del Derecho Internacional ,el Convenio de Ginebra del 22 de Agosto de 1864 (FOSSATI, (2017), p 28).

CONCEPTUALIZACION DEL DEREHO INTERNACIONAL HUMANITARIO

Así las cosas el Derecho Internacional Humanitario puede ser definido como el conjunto de normas cuya finalidad, en tiempo de conflicto armado es, por una parte, proteger a las personas que no participan, o han dejado de participar, en las hostilidades y, por otra, limitar los métodos y medios de hacer la guerra.

En otros terminos, por Derecho Internacional Humanitario aplicable en los conflictos armados, el Comité Internacional de la Cruz Roja, entiende que incluye a las normas internacionales, de origen convencional o consuetudinario, especialmente destinadas a solucionar los problemas de índole humanitaria que se derivan directamente de los conflictos armados, internacionales o no, y limitan, por razones humanitarias, el derecho de las partes en conflicto a utilizar los métodos y medios de hacer la guerra de su elección teniendo como finalidad la protección de las personas y los bienes afectados o que pueden verse afectados por el conflicto bélico, comprendiendo dos ramas distintas, el Derecho de Ginebra, cuyo objetivo es proteger a los militares que han dejado de participar en los combates y a las personas que no participan directamente en las hostilidades, por ejemplo, la población civil y por otro lado, el Derecho de La Haya, por el que se determinan los derechos y las obligaciones de los beligerantes en la conducción de las operaciones militares. (CICR, (2005), p 4/5).

A partir de la noción de Derecho Internacional Humanitario y las finalidades específicas perseguidas por éste, se han formulado distintos principios elaborados en primer lugar por Jean Jactes Rosseau, Frederic De Martens y, posteriormente enunciados taxativamente en el Preámbulo de la Declaración de Petersburgo de 1868, la que tuvo por objeto prohibir el uso de determinados proyectiles en tiempo de guerra.

PRINCIPIOS DEL DERECHO INTERNACIONAL HUMANITARIO

Los siguientes postulados son lo que la doctrina ha caracterizado como los principios del Derecho Internacional Humanitario entre los que se encuentran el principio de limitación, principio de necesidad militar, principio de humanidad, principio de distinción y principio de proporcionalidad, agregándose por algunos autores el principio de protección al medio ambiente siendo definidos todos estos como aquellas directrices universales, reconocidas por las naciones civilizadas obligatorias para los Estados más allá de un vínculo convencional, que pueden abstraerse de las normas contenidas en los Convenios de Ginebra y sus Protocolos Adicionales, e inspiran esta particular rama del Derecho y determinan, limitan y encauzan el comportamiento a seguir por los intervinientes en un conflicto armado para cumplir con las finalidades perseguidas por el Derecho Internacional Humanitario y, por lo mismo, orientan su interpretación y aplicación (López Díaz, (2009), p 2).

Tomamos por su claridad expositiva, las definiciones elaboradas en el Libro de Derecho Internacional Humanitario elaborado por el Ministerio de Defensa, lugar donde cada uno ha sido definido de la siguiente manera:

Principio de necesidad militar: Toda actividad de combate debe justificarse por motivos militares; están prohibidas las actividades que no sean militarmente necesarias. Está prohibido atacar a pacíficas personas civiles o quienes estén fuera de combate, porque con ello no se obtiene ventaja militar alguna. En las normas de los tratados internacionales se tiene debidamente en cuenta la necesidad militar. No se puede invocar como excusa la necesidad militar para invalidar el derecho de los conflictos armados. Toda acción emprendida para destruir bienes del enemigo y requerida por la necesidad militar tiene que avenirse con los principios de distinción y de proporcionalidad. No se puede recurrir a la necesidad militar como excusa para la dejadez, la indiferencia o el comportamiento no profesional.

Principio de limitación: En todo conflicto armado, el derecho de las partes en conflicto a elegir los métodos o medios de combate no es ilimitado.
Queda prohibido el empleo de armas, proyectiles, materiales y métodos de tal índole que causen males superfluos o sufrimientos innecesarios, como tambien asi el empleo de métodos o medios que hayan sido concebidos para causar, o de los que quepa prever que causen daños extensos, duraderos y graves al medio ambiente natural.

Principio de proporcionalidad: Dado que los métodos o medios no son ilimitados, los ataques, es decir los actos de violencia contra el adversario, sean ofensivos o defensivos, no podrán ser indiscriminados ni excesivos en relación con la ventaja militar concreta y directa prevista.

Principio de buena fe: Ha de prevalecer la buena fe en las negociaciones de los beligerantes.

Principio de prohibición de represalias: Se prohíben las represalias, es decir las violaciones del derecho como respuesta a otras violaciones del derecho contra los heridos, los enfermos y los náufragos, el personal sanitario y los servicios sanitarios, el personal y los servicios de protección civil, los prisioneros de guerra, las personas civiles, los bienes civiles y culturales, el medio natural y las obras e instalaciones que contienen fuerzas peligrosas.

Principio de subsidiariedad (Regla de Martens): En los casos no previstos en los Convenios, en el Protocolo o en otros acuerdos internacionales, o en caso de denuncia de esos acuerdos, las personas civiles y los combatientes quedan bajo la protección y el imperio de los principios del derecho de gentes derivados de los usos establecidos, de los principios de humanidad y de los dictados de la conciencia pública".

Principio de distinción: La aplicación del principio de distinción exige definir claramente las personas y los bienes que es lícito atacar. Por lo que respecta a las personas, los combatientes del enemigo son miembros de las fuerzas armadas de una parte en un conflicto (salvo el personal médico y los capellanes). Las personas que no sean miembros de las fuerzas armadas son civiles y, por ende, no deben ser objeto de

los ataques. Sin embargo, hay una excepción: es lícito atacar a los civiles que participan directamente en las hostilidades, sea en forma individual o como parte de un grupo, aunque sólo mientras dure su participación directa en las hostilidades (Ministerio de Defensa, (2010), p 24-26).

CONCEPTUALIZACIÓN DE CIBERESPACIO

Habiendo caracterizado al Derecho Internacional Humanitario, definido sus principios y para la temática que se analiza, resulta necesario caracterizar al Ciberespacio definido como: un nuevo ambiente en donde el ser humano realiza infinidad de actividades, entre las que se pueden citar el correo electrónico, el comercio, lectura, entretenimiento, administración, investigación, desarrollo y diseño en innumerables disciplinas; redes sociales; navegación; comunicaciones, defensa y seguridad cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicaciones (BARRETO, (2017), p. 7- 8).

Puede entenderse que el ciberespacio puede ser caracterizado como un espacio complejo donde en la actualidad interactúan no sólo organizaciones públicas, privadas sino la humanidad en su conjunto, su importancia radica en que es un lugar abstracto pero no por ello sin importancia ya que se desarrollan múltiples actividades vitales donde en caso de producirse una grave afectación el daño ocasionado recae en toda la sociedad.

CIBERGUERRA

En este sentido una de las formas de afectación es a través de la ciberguerra la cual ha sido definida una agresión promovida hacia un estado con la finalidad de dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de dato pero con la característica principal que el medio empleado no será la violencia física sino un ataque informático que va desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento (SANCHEZ MEDERO, (2010) p. 64).

Analizando a este fenómeno parte de la doctrina entiende que todavía no se ha producido un ataque de gran impacto y muchos se aventuran a pronosticar que la guerra del Siglo XXI se librará en el ciberespacio, aunque, si bien no han existido ataques de magnitud, se han registrado distintos ataques informáticos que recibieron el nombre de ciberguerra como los ataques que se produjeron durante la Guerra de Kosovo, Taiwán que se caracterizaron por su magnitud, no obstante lo manifestado, el caso

paradigmático, fue el ataque cibernético sufrido por Estonia en el Año 2007 donde se afectaron distintos medios de comunicación, bancos y diversas entidades e instituciones gubernamentales luego del anuncio del gobierno estonio de realizar excavaciones en la Plaza de Tonismäe, ubicada en Tallin su capital, con el propósito de identificar restos de soldados caídos durante la Segunda Guerra Mundial y trasladarlos al cementerio militar de Tallin.

Semejante decisión, incluía el traslado de la estatua conocida como el soldado de bronce erigida en la entrada del cementerio militar de Tallin, e instalada en 1947 por los soviéticos con motivo de su victoria sobre el ejército nazi (Ferrrero, (2013), p 83).

Los ciberataques tuvieron lugar entre el 27 de abril y 18 de mayo del 2007,durante este periodo variaron su objetivo, su volumen y método, pero en líneas generales se pueden considerar dos fases: la primera fase tuvo lugar entre el 27 y 29 de abril; en ella se emplearon herramientas de ciberataque rudimentarias por parte de hacktivistas sin grandes conocimientos técnicos emplazados en sitios web, mayoritariamente rusos, contra sitios web de Estonia, especialmente del Gobierno, del Ministerio de Defensa y de los principales partidos políticos. La alarma surgió cuando reunido el Gobierno Estonio observó que no podía cargar los comunicados de prensa en sus sitios web oficiales. Una vez confirmado que el país se encontraba bajo un ciberataque, el Gobierno procedió de una manera inmediata a organizar un equipo de respuesta, liderado y coordinado por el Equipo Nacional de Respuesta ante Incidentes Informáticos (Estonian-CERT), compuesto por personal experto de los Ministerios de Comunicaciones de Defensa y los Servicios de Inteligencia. En la segunda fase del ataque cibernético que transcurrió entre el 30 de abril hasta el 18 de mayo, la arremetida se volvió más compleja, con uso de grandes botnets con una coordinación minuciosa y precisa

CONCLUSIONES

Mencionamos y caracterizamos a este caso porque fue la primera vez donde un estado perteneciente a la OTAN solicitó apoyo a los países miembros de esta organización por un ataque a sus sistemas de información y porque fue el hito que impulsó un manual de derecho internacional que se denominó el Manual del Tallin, que fue dirigido por el Profesor Michael Schmitt de la US Naval War College, y que se presentó en Londres el 15 de marzo de 2013. La premisa fundamental con la que se empezó a redactar este Manual fue que la guerra no deja de ser tal porque se lleve a cabo en el ciberespacio, es decir, es posible la guerra en el ciberespacio (Reguera Sánchez, (2015), p 14).

Así el Manual intenta ser una herramienta para los juristas que quieran tener una visión global de los desafíos jurídicos internacionales relacionados con la conflictividad en el ciberespacio, el cual se encuentra estructurado en noventa y cinco reglas dispuestas en dos partes, la seguridad del ciberespacio en el Derecho Internacional y el Derecho

Internacional de los conflictos armados, todas ellas reflejan el consenso existente en esta materia y van acompañadas de comentarios que incluyen las fuentes utilizadas y aportan un análisis detallado de la lógica seguida en su redacción (Reguera Sánchez, (2015), p 15).

Habiendo mostrado los antecedentes de la ciberguerra corresponde determinar si los principios del DICA se aplican a la ciberguerra, así se ha expresado que ésta constituye uno de los retos más latentes del Derecho Internacional Humanitario, ya que presenta una serie de figuras que anteriormente no habían sido visualizadas en el DIH tales como la violación de la soberanía estatal, la regulación del ciberespacio, la vulneración de los principios del DIH y los ataques a la población civil de manera indiscriminada, así hasta la aparición de internet, las guerras se habían llevado a cabo en los espacios terrestre, marítimo, aéreo, espacial y ciberespacial. Es a partir de la década de los 90 cuando la consolidación del crecimiento de la infraestructura tecnológica y el uso de las redes, hacen que cada vez se vea más al ciberespacio como un nuevo campo de batalla, donde se lleve a cabo la ciberguerra (SUAREZ. (2016), p 32).

En aspecto de lo señalado, el Comité de la Cruz Roja Internacional tomando en cuenta los informes presentados por el Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los Avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, entendió que el Derecho Internacional Humanitario, y en particular, la Carta de las Naciones Unidas es aplicable al ciberespacio. Así el Grupo de Expertos dependiente de la Organización las Naciones Unidas entendió que en los ciberconflictos se deben observar todos los principios y normas del DIH, como sucede con cualquier otra arma, medio o método de guerra, nuevo o antiguo, no haciendo ninguna diferencia en el hecho que el ciberespacio se considere un nuevo dominio para la guerra similar al aire, la tierra, el mar y el espacio exterior (CICR, (2015), p 52).

Desde otro punto de vista, la Corte Internacional en su Opinión Consultiva acerca de la licitud de la amenaza o del empleo de armas nucleares, recordó que los principios y normas establecidos en el derecho humanitario aplicable a los conflictos armados se aplicaban a todas las formas de la guerra y a todos los tipos de armas, incluso a las del futuro. Esto también queda claro en el Artículo 36 y 49 del Protocolo Adicional I de Ginebra ya que ambos demuestran la pretensión internacional sobre la aplicación de las normas de la guerra terrestre a todo tipo de conflicto bélico que pudiese afectar bienes o derechos de los civiles. En este sentido, no caben dudas de que la guerra cibernética se librará al menos parcialmente desde infraestructuras situadas en tierra contra objetivos en tierra, y que plantea el riesgo de afectar a los civiles en tierra (CICR, (2015), p 53).

Resulta importante destacar la opinión en la materia de la Dr.Grispo quien expresó que: *"(…) Las ciberoperaciones en sí mismas no tienen por qué producir un conflicto armado entre las partes o una hostilidad, pero en cambio los ciberataques pueden dar lugar a*

un conflicto armado entre dos partes organizadas. Así el Derecho Internacional Humanitario sólo entra en juego cuando las operaciones cibernéticas se cometen en el marco de un conflicto armado, sea entre estados, entre estados y grupos armados organizados, o entre grupos armados organizados. Las ciberoperaciones pueden originar un conflicto armado, cuando estas originan una hostilidad entre varias partes con intereses contrapuestos y pueden derivar en un ciberataque, cuando la ciberoperación lleva implícita el uso de la fuerza, entendida de esta manera se refiere también que la ciberguerra se da en un ámbito, el ciberespacio, que goza de sus propias características, que no contempla el Derecho Internacional". (GRISPO, (2016), p 2).

Finalmente hemos analizado que la ciberguerra constituye un nuevo desafío para el Derecho Internacional de los Conflictos Armados que se librará en un ambiente que se caracteriza por su indeterminación y abstracción y donde las amenazas no solo pueden provenir de naciones sino también de estados fallidos, grupos terroristas por ser los ciberataques un medio rápido, económico y ágil que, vulnera la seguridad de una nación de manera sensible. Este fenómeno implica la impulsión de distintas normas internacionales que regulen al ciberespacio tomando como antecedente los principios que se encuentran en el Manual del Tallín.

BIBLIOGRAFÍA.

CRUZ ROJA INTERNACIONAL; (2005); El Derecho Internacional Humanitario; Disponible en: https://www.icrc.org/es/doc/assets/files/other/icrc_003_0703.pdf

BARRETO, Juan F; (2017); Tesis: La Defensa Nacional y la estrategia militar de seguridad cibernética; Disponible en:http://www.cefadigital.edu.ar/bitstream/123456789/1061/1/TFM%2004-2018%20BARETTO.pdf.

CARDONA, Vanesa; (2008); Derecho Internacional Humanitario: Verdades y contradicciones; Disponible en http://www.redalyc.org/articulo.oa?id=85550913

CRUZ ROJA INTERNACIONAL; (2015); El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos; Disponible en: https://www.icrc.org/es/download/file/15128/32ic-report-on-ihl-and-the-challenges-of-armed-conflicts_es.pdf.

FERRERO, Julio; (2013). La ciberguerra. Génesis y Evolución. Disponible en: https://kipdf.com/la-ciberguerra-genesis-y-evolucion_5b1698fd7f8b9a1a568b4602.html

FOSATI, Jorge; (2017); Vigencia del derecho internacional humanitario en la actualidad en el marco de la conducción de operaciones militares en el nivel operacional;

Disponible en: http://www.cefadigital.edu.ar/bitstream/123456789/1165/1/TFI%2013-2017%20FOSSATI.pdf

GRISPO, Matilde; (2016); Derecho internacional y seguridad cibernética; Disponible en: http://www.cefadigital.edu.ar/bitstream/123456789/853/1/VC%2016_GRISPO.pdf

LÓPEZ DÍAZ, Patricia; (2009); principios fundamentales del Derecho Internacional humanitario; Disponible en: https://revistamarina.cl/revistas/2009/3/lopez.pdf

MINISTERIO DE DEFENSA; (2010); Manual de Derecho Internacional Humanitario.

MOSSO, Juan M; (2015); Ciberseguridad Inteligente; Disponible en: http://www.bacchuss.com.ar.

PALACIO, Juan E; (2013); Evolución del Ejército Argentino en seguridad informática en el marco de operaciones militares llevadas a cabo en el ciberespacio; Disponible en:http://www.cefadigital.edu.ar/bitstream/123456789/551/1/TFL%20LEO%202013%20P1E5_96.pdf.

SANCHEZ MEDERO, Gema; (2010); Los Estados y la Ciberguerra; Disponible en: https://dialnet.unirioja.es/descarga/articulo/3745519.pdf

SUAREZ VIVES, Maryam; (2015); La ciberguerra y la aplicación de los principios del Derecho Internacional Humanitario; Disponible en: http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/1953/1/suarez_vm.pdf

STEL, Enrique; (2005); Guerra Cibernética. Buenos Aires: Círculo Militar

REGUERA SANCHEZ, Jesús; (2015); Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario; Disponible en : http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario.