PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Ciberterrorismo: Un nuevo desafío para el Derecho Internacional Humanitario

TRABAJO DE INVESTIGACIÓN PARA OBTENER EL

GRADO DE BACHILLER EN DERECHO

AUTOR

Paredes Puente de la Vega, María Graciela

ASESOR

Novak Talavera, Fabián Martin Patricio

2021

RESUMEN

El ciberespacio es un escenario nuevo de confrontación con el terrorismo, un escenario que requiere una mirada distinta por parte del Derecho Internacional y es que, sobre la materia, surgen varias dudas, sin embargo, la columna vertebral del presente artículo se limita a contestar solo a una: ¿Los ataques de ciberterrorismo perpetrados por el DAESH se encuentran previstos en la definición de terrorismo y por ende, encuentran regulación en el Derecho Internacional Humanitario? Para responderla será necesario abordar, en primer lugar, la problemática para el consenso en la definición de terrorismo, ya que a partir de ella y del análisis de la doctrina y jurisprudencia se podrán desarrollar las características principales del fénomeno con el fin de contar con una definición propia. En segundo lugar, es menester analizar la regulación desde la perspectiva del Derecho Internacional Humanitario, es decir, lo que se señala sobre el fenómeno desde el Derecho de Ginebra. Finalmente, y con el panorama claro, se dara paso al tercer punto, el que busca explicar al ciberterrorismo como una nueva modalidad terrorista. Todo el análisis anterior sirve para apoyar una única respuesta y es que finalmente los ataques de ciberterrorismo perpetrados por el DAESH sí se encuentran previstos en la definición de terrorismo, y con ello, tienen regulación desde el Derecho Internacional Humanitario.

ABSTRACT

Cyberspace is a new scenario of confrontation with terrorism, a scenario that requires a different perspective of International Law and is that point several doubts arise, however, the mainstay of this article is limited to answering only one of those question: Are the cyberterrorist attacks perpetrated by the DAESH included in the definition of terrorism and therefore have regulation in International Humanitarian Law? In order to answer this question, it will be necessary to address, first of all, the problem of reaching a consensus on the definition of terrorism, since it is on the basis of this definition and an analysis of the doctrine and case law that the main characteristics of the phenomenon can be developed in order to have a definition of its own. Secondly, it is necessary to analyze the regulation from the perspective of International Humanitarian Law, that is, what is indicated about the phenomenon from the Law of Geneva. Finally, and with a clear overview, we will move on to the third point, which seeks to explain cyberterrorism as a new form of terrorism. All of the above analysis serves to support a single response, and that is that finally the cyberterrorist attacks perpetrated by the DAESH are included in the definition of terrorism, and therefore are regulated by International Humanitarian Law.

ÍNDICE DE CONTENIDO

Ciberterrorismo: Un nuevo desafío para el Derecho Internacional Humanitario

1. Introducción

El presidente de Estados Unidos, Donald Trump, señaló el día 20 de marzo de 2019 que el Estado Islámico "habrá desaparecido esta noche" de Siria. Lo anunció en un encuentro con periodistas, mientras mostraba una hoja con dos mapas del país, el de arriba, supuestamente, mostraba en color rojo las zonas controladas por el DAESH en Siria en 2016 cuando llegó a la presidencia; y, el de abajo, con la coloración prácticamente inexistente, referida a la presencia del grupo terrorista en el país. Ante esto afirmó: "Cuando asumí el mando, era un desastre. Ahora, añadió, no hay rojo" (Guimón, 2019). No es la primera vez que Trump declara la inminente derrota del autoproclamado califato. Suyas son frases como: "Acabamos de recuperar el 100% del territorio controlado por Daesh en Siria" o "[…] En el plazo de "una semana" los pocos reductos que todavía quedan habrán sido borrados del mapa" (Guimón, 2019).

La cuestión es: ¿está o no finalmente derrotado DAESH? Según Patrick Cockburn (2019), corresponsal en Oriente Medio del *Financial Times* y de *The Independent*, al debatir la desaparición o supervivencia del DAESH, los especialistas caen en la misma omisión notoria, pues ignoran el hecho de que el baluarte más grande resulta el enclave yijadista en la provincia de Idlib, que retiene en su poder la *Hayat Tahrir al-Sham* (HTS), una poderosa facción escindida del DAESH que fundó el grupo con el nombre de *Jabhat al-Nusra* en 2011 y con la que comparte las mismas creencias fanáticas y tácticas militares.

Es decir, siguiendo en este razonamiento a David Rapoport (2004) cuando señala que el terrorismo moderno comenzó en 1879 y ha existido durante los ciento veinticinco años siguientes y que, durante este tiempo hemos

experimentado cuatro oleadas de terrorismo, siendo la última de ellas, la del terrorismo religioso; no es descabellado pensar que el fenómeno terrorista no desaparece, sino que en realidad, se transforma con relación a su época.

Quizá es esa la verdadera razón por la que Trump señala que el califato desaparece pues, sin lugar a dudas, lo hace tal y como lo conocemos; las prácticas de terror de Al Qaeda quedaron desplazadas por los primeros vídeos que el DAESH hizo viral ¿Por qué? Porque era un terror que no conocíamos, porque la escala de deshumanización que mostraron al mundo no tuvo pausas y, porque aunque el DAESH ya no exista la historia presagia que este fenómeno no acaba, por lo que debemos ser capaces de responder a los desafíos que nos genera el constante cambio del que somos parte, y es que el ser humano a lo largo de la historia, siempre ha buscado fórmulas para saber a qué se enfrentará para poder tener las respuestas adecuadas a las circunstancias.

Con la aparición de DAESH y su capacidad sin precedentes para desenvolverse en el ciberespacio, se abre un mundo de posibilidades para entender el fenómeno terrorista, pues ya dejamos atrás ataques como el del 11 de setiembre; ahora el desafío está íntimamente conectado con ese influjo de información que alberga el ciberespacio.

En palabras simples, cambiamos de escenario, estabamos acostumbrados a un terrorismo de bombas y terror palpable, un terror de muertos y heridos; y ahora aunque este no ha desaparecido, nos enfrentamos a uno nuevo, a ataques en la red y terror psicológico.

Llegados a este punto las interrogantes comienzan a aparecer y es lógico, el ser humano, siempre ha buscado maneras que le permitan predecir el futuro, y aunque no hay posibilidad alguna de asegurar lo que nos depara, este trabajo tiene como objetivo general alinearse con muchos otros que

como yo, tienen la intención de generar reflexión sobre los desafíos actuales que tiene el Derecho Internacional Humanitario (en adelante DIH)

Pero, más allá de la reflexión, es primordial contar con objetivos más concretos, más específicos, como, por ejemplo: brindar un panorama de la normativa del DIH que tiene relación con el fenómeno del terrorismo y definir el fenómeno del ciberterrorismo, a través del entendimiento de conceptos como ciberespacio y acto terrorista.

Sumado a lo anterior, y con una mayor importancia para la investigación, afirmar si el ciberterrorismo es parte del fenómeno terrorista; por lo que, cuando el DIH prohíbe el "terrorismo" lo hace en todas sus esferas, siendo una de ellas, la del ciberespacio; este objetivo tendrá su desarrollo a partir de la respuesta a la columna vertebral del presente artículo:

¿Los ataques de ciberterrorismo perpetrados por el DAESH se encuentran previstos en la definición de terrorismo y por ende, encuentran regulación en el DIH?

2. Marco teórico-normativo

Para dar respuesta a la interrogante mencionada al final del apartado anterior es imprescindible que se clarifiquen ciertos conceptos entre los que se encuentran:

2.1 El Ciberespacio

Sobre este concepto, es importante, en primer lugar, mencionar que según indica Urueña Centeno (2015, pp. 4-5) y el informe de la Agencia Europea para la Seguridad de las Redes y de la Información (*ENISA,* en sus siglas en inglés) del año 2017, las amenazas más relevantes en el ciberespacio son, entre muchas otras: *malware*, ataques basados en el uso de la web, ataques basados en aplicaciones web, denegación de

servicio, *botnets, phishing*, correo basura (*spam*), *ransomware*, amenaza interna, daños físicos, robos o pérdidas, kit de explotación de vulnerabilidades, violación de datos, robo de identidad, fuga de información y ciber-espionaje.

Teniendo en cuenta que las amenazas anteriormente descritas difieren unas de otras y que el fin del presente trabajo es comprender el ciberterrorismo, es primordial clarificar, primero, el medio utilizado para los ataques.

Respecto a ello, la doctrina afirma que el ciberespacio debe ser entendido como un espacio de interacción, es decir, básicamente como un espacio-sistema relacional, y es que a diferencia de otro tipo de espacios que pueden ser utilizados para distintas funciones, pero que tienen una naturaleza física primaria; el ciberespacio surge directamente como un espacio relacional. Dos personas pueden encontrarse en un lugar y comenzar en ese momento una relación, pero ese espacio ya existia y seguirá existiendo después de que esa relación termine. Por otro lado, este espacio virtual existe solamente como espacio relacional; su realidad se construye a través del intercambio de información, es decir, es espacio y es medio (Aguirre, 2004).

Sumado a lo anterior, el concepto emanado del Departamento de Defensa de los Estados Unidos (2016), es bastante claro al señalar que el ciberespacio es:

> *Un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información (incluyendo internet), redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores*.

Además, José Ramón Casar (2012, p.15) define al ciberespacio desde un enfoque de defensa, como aquel espacio estratégico para el que hay que definir medidas de prevención, disuación, protección y reacción; siendo sus características diferenciales del resto de los espacios las siguientes:

> *1. El ciberespacio es un entorno único, en el que el atacante puede estar en cualquier parte del globo.*
>
> *[…] 3. La confrontación en el ciberespacio presenta frecuentamente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.*
>
> *4. Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema, y a menudo sin delatarse.*
>
> *[…] 6. Evoluciona rápidamente siguiendo la evolución tecnológica de las TIC.*

Por todo lo antes señalado, para efectos de la investigación considero que la definición de Joaquín Aguirre, es la que más se ajusta al objetivo de la investigación, pues él centra su enfoque en la interacción que es inherente a este nuevo escenario de conflicto, mientras que otras definiciones rozan el exceso técnico propio de la informática o cuentan con un enfoque de estrategia de defensa.

Además, teniendo en cuenta la velocidad en la que la tecnología avanza, una definición tan amplia como la que se señala es vital para evitar el desfase.

Ahora bien, es importante mencionar sobre este concepto que hay quienes parten del hecho que el acceso a las tecnologías de la información y por ende al ciberespacio, debe entenderse como un

derecho, ya que son muchos los Estados en los que el acceso a la red se reconoce como tal.

Así, por ejemplo, en Finlandia se reconoció en 2010 el “derecho humano fundamental a internet de banda ancha” (Reguera, 2015), así es evidente para ellos que se debe proteger el libre uso del mismo en condiciones de libertad y seguridad. Sin embargo, la pregunta que surge es ¿Cómo es el acceso al ciberespacio? ¿Es libre? ¿Es regulado? ¿Cúal se prefiere? Ya que las respuestas a estas interrogantes exigen la toma de posición y una explicación más detallada, se verán en el apartado correspondiente al Desarrollo.

2.2 Ciberterrorismo

Respecto a este concepto, Masana (2002, p. 12) afirma que este fue acuñado en los años 80 por Barry Collin, un investigador senior del *Institute for Security and Intelligence* para referirse a la convergencia del ciberespacio con el terrorismo. Sin embargo, es recién con Mark Pollit que se desarrolló una definición operativa mucho más completa:

> *El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos*

En la línea de lo antes mencionado, Dorothy E. Denning en el *Special Oversight Panel on Terrorism, Committee on Armed Services* de la cámara baja estadounidense, en el año 2000 explica que para ser calificado como ciberterrorismo un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo.

Ejemplos válidos de lo mencionado serían los ataques que deriven en muertes o personas heridas, explosiones, colisiones de aviones, contaminación de agua o severas pérdidas económicas.

Por otro lado, gracias al análisis de los alcances de los medios informáticos en acciones delictivas Urueña Centeno delimita al ciberterrorismo partiendo de la definición de un delito informático, como toda aquella acción ilegal que se dá por las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet (2015, p. 2).

Esto en razón de que en nuestros días, la preparación y ejecución de casi la totalidad de acciones terroristas están apoyadas cibernéticamente o utilizan en algún momento medios cibernéticos en su realización tanto para comunicación como para la propia acción.

De otro lado, Chicharro Lázaro (2013) define ciberterrorismo como: “el uso de las nuevas tecnologías con fines terroristas”. Entonces, para la autora los terroristas pueden usar las herramientas informáticas como objeto para ocasionar daños lanzando ataques de cualquier tipo contra equipos informáticos, redes o información recogida en ellas.

De la misma manera, para Pons Gamón estamos ante una realidad en la que se pueden ejecutar atentados terroristas a través del empleo de cualquier acción contra los sistemas y redes, causando en muchos casos daños físicos y, por último; pueden servirse de internet para su propaganda, incitación, amenazas, financiamiento de ataques y reclutamiento (2017).

Si nos referimos al uso que los terroristas hacen en este nuevo espacio, hay que indicar, tal y como refiere Conway (2006, p. 7), que el internet

tiene la capacidad de conectar no solo a miembros de las mismas organizaciones terroristas, sino también a miembros de diferentes grupos.

Así, por ejemplo, existen sitios “yihadistas” en todo el mundo que expresan su apoyo al terrorismo, y en su web permiten que terroristas en lugares tan lejanos como Chechenia, Indonesia, Turquía, Irak, Filipinas, Líbano, entre muchos otros, intercambien no solo ideas y sugerencias, sino también información práctica sobre cómo construir bombas, establecer células terroristas y, perpetrar ataques (p.7).

Sumado a lo mencionado, el Consejo de Europa define el ciberterrorismo como aquel “terrorismo que utiliza las tecnologías de la información para poder intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos” (Subijana, 2008, p. 172). Es decir, los ataques del ciberterrorismo que responden a una motivación ideológica, muchas veces tienen la intención de causar pánico colectivo y, esto exige abrir el panorama, comenzando a replantear la seguridad nacional y las políticas de defensa.

Analizando las ciberamenazas terroristas, para Olier Arenas los ataques son cada vez más sofisticados y afectan redes informáticas que en teoría disponen de niveles de seguridad extremos (2013, p. 9).

En vista de todo lo anterior, considero fundamental no solo contar con una definición amplia de ciberterrorismo, sino que debe emerger de un profesional de prestigio, que sea reconocido en el ámbito académico. Por ello, y al ser la definición de Alicia Chicharro Lázaro la que cumple con ambas condiciones, será la definición guía en la presente investigación.

Pero, ¿Por qué es importante contar con una definición de ciberterrorismo? Pues, al ser este concepto el eje central de la presente investigación, es evidente su importancia.

Lejos de las definiciones, es menester aclarar la diferencia que existe entre ciberterrorismo y hacktivismo. Según Pérez (2020, p. 5) el término hacktivismo, surge de la combinación de *hacking* y activismo, entendiéndose como una articulación entre el activismo y el uso de las herramientas hacker para protestar en Internet; es decir, el uso ilegal o legal de herramientas digitales para fines políticos y de protesta, es decir, se limita al ciberataque y no a todo el fenómeno detrás del mismo.

Incluso, Pino (2014) lo considera como un ejemplo leve de *Netwar*, por lo que el autor no lo interpreta como una acción criminal, sino más bien como una forma legítima de protesta.

2.3 Terrorismo

Llegados a este punto, es claro que todas las definiciones de ciberterrorismo antes señaladas nos remiten al macro-concepto, es decir, a la definición de terrorismo.

Para poder entender este concepto es importante partir de la idea que, para el Informe del Grupo de Alto Nivel sobre las amenazas, los desafíos y el cambio (2004) que se encuentra recogido en el documento A/59/565 de la Asamblea General de Naciones Unidas, prácticamente todas las formas de terrorismo están prohibidas por uno de los 12 convenios internacionales contra el terrorismo, el derecho consuetudinario internacional, los Convenios de Ginebra y el Estatuto de Roma.

Sin embargo, el informe señala también, que la falta de consenso sobre una definición clara de terrorismo compromete la posición normativa y moral contra el mismo, es decir, ¿cómo vamos a condenar una acción si no estamos seguros de lo que calza en ese macro-concepto?

Walter Laqueur (1987, p. 143), quién sostuvo que una sola definición de terrorismo no es suficiente para describir dicha actividad, trata de explicarlo como:

> *el uso o la amenaza de uso de la violencia, un método de combate, o una estrategia para conseguir ciertos objetivos (…) pretende infundir en las víctimas un estado de miedo, que es despiadado y se encuentra al margen de toda regla humanitaria (…) la propaganda, es un factor esencial en la estrategia terrorista.*

De la misma manera, para Reinares (2003, pp. 16-17), hablar de terrorismo es hablar de violencia, de una violencia caracterizada fundamentalmente porque el impacto psíquico que provoca en una determinada sociedad supera ampliamente las consecuencias puramente materiales. Es una violencia sistemática e imprevisible, practicada por actores individuales o colectivos y dirigidos contra objetivos vulnerables que tienen alguna relevancia simbólica en sus correspondientes entornos culturales o marcos institucionales.

Por otro lado, Hoffman define el terrorismo como la creación deliberada y la explotación del miedo mediante la violencia o amenaza de violencia, cuyo objetivo es el cambio político, es decir; pone énfasis en que el terrorismo está especialmente diseñado para tener efectos psicológicos a largo plazo, más allá de las víctimas inmediatas o del objetivo primero de sus atentados (1999, p. 63).

Ahora bien, para Alex Schmid (2012) estudioso sobre terrorismo y ex oficial a cargo de la Subdivisión de Prevención del Terrorismo de las Naciones Unidas, la definición de terrorismo debe: a) señalar que es una doctrina o práctica, b) hacer referencia al contexto en el que el terrorismo se emplea como técnica, c) incluir el concepto de violencia física o

amenaza de la misma, información sobre procesos de comunicación basados en la amenaza, d) mencionar que el terrorismo produce miedo, pánico, ansiedad, etc, e) decir algo sobre las víctimas, puntualizando que no son el fin último, f) señalar algo sobre los perpetradores, g) indicar que el terrorismo es predominantemente político y h) incluir las intenciones de los actos terroristas, la motivación para unirse y dejar en claro que todo forma parte de una campaña de violencia.

En contraste, el Departamento de Defensa de los Estados Unidos, define el terrorismo como: “el uso calculado de la violencia o de la amenaza de violencia contra individuos o propiedades para infundir miedo, con la intención de coaccionar o intimidar al gobierno o a sociedades para conseguir objetivos políticos, ideológicos o religiosos” (2000).
En similar línea, la OTAN define el terrorismo en su publicación AAP-6 como: “uso o amenaza de uso ilegal de la fuerza o de la violencia contra personas o propiedades con la intención de coaccionar o intimidar a gobiernos o sociedades para conseguir objetivos políticos, religiosos o ideológicos” (2016).

Con relación a la Organización de Naciones Unidas (ONU) la Resolución 49/60/1995 de la Asamblea General de Naciones Unidas define al terrorismo como: “actos criminales con fines políticos concebidos o planeados para provocar un estado de terror en la población en general”.

En la Resolución 51/210/1999 de la Asamblea General de Naciones Unidas el enfoque cambia, ya que el terrorismo es definido como: “acto criminal que pretende provocar un estado de terror en la población, en un grupo de personas, o en personas determinadas, para conseguir objetivos políticos”.

Asimismo, entre las principales resoluciones relativas al terrorismo aprobadas por el Consejo de Seguridad en virtud del Capítulo VII de la Carta se encuentran: 1540 (2004), 2170 (2014), 2178 (2014), 2199 (2015) y 2253 (2015).

También los propios terroristas han intentado definir sus acciones, aunque claro siempre en busca de su propio beneficio. Algunos grupos se autodenominan "ejército" con la clara intención de despojarse de la etiqueta "terrorista" y de apartar la idea de ilegalidad a sus acciones. Así, por ejemplo, encontramos el IRA (Irish Republican Army), el Nuevo Ejército del Pueblo de Filipinas, el Ejército de Liberación Nacional (ELN) de Colombia, el Ejército de Liberación de Ruanda, el Ejército Rojo Japonés y muchos otros (Orti, 2012, p. 17).

En consecuencia, con relación a esta definición ha quedado sentado que no hay consenso sobre ella, y tal como se encuentra previsto en la presente investigación, se buscará aportar una propia. Por lo tanto, para alcanzar nuestro objetivo resulta de suma utilidad las características a las que alude Alex Schmid.

Ahora bien, para poder vincular el ciberterrorismo y el DIH, lo que es medular en la presente investigación, es necesario revisar aquello que existe sobre la relación entre el concepto de terrorismo y el DIH.

El moderno derecho de los conflictos armados se encuentra conformado por los cuatro Convenios de Ginebra de 1949 y por los Protocolos Adicionales I y II de 1977, que complementan a los primeros.

Además, este conjunto normativo se rige por dos grandes principios, a saber:

(a) El principio de la discriminación, que tiene por objetivo hacer dos grandes distinciones. Por un lado, los objetivos militares y bienes civiles y, por otro lado, los “combatientes” y población civil.

(b) El principio de proporcionalidad, en virtud del cual se encuentran prohibidas las acciones militares cuyo daño excedan las ventajas militares que puedan obtenerse.

A los principios generales antes señalados se suma la regla contenida en la llamada cláusula Martens, la cual indica que, en ausencia de una prohibición específica, debe hallarse una norma compatible con los principios de humanidad y los dictados de la conciencia pública (Díez de Velasco, 2001, p. 871).

En consecuencia, el terrorismo en sí mismo es contrario a los principios del DIH. No obstante, esta afirmación es válida, para cierto sector de la doctrina, en la medida que tal delito se cometa en el marco de un conflicto armado.

En contraposición a ello, para Elisabetta Cutrale (2019, p.96), los miembros del DAESH se han distinguido de otros grupos terroristas por "el efectivo control del territorio conquistado", por lo que deberían ser considerados "parte" de un conflicto conforme a las Convenciones de Ginebra, sus protocolos adicionales y lo más importante, conforme a los objetivos de la jurisdicción internacional en el caso de actos de violencia contra la población civil. Para la autora, el elemento de la territorialidad del DAESH permite necesariamente delinear una nueva categoría jurídica, un tipo de "híbrido" entre las comunes definiciones jurídicas de "conflicto interno" y "conflicto internacional", lo que permitiría dejar de lado el análisis del conflicto armado entendido solo como los compartimentos limitados de CAI y CANI para el terrorismo.

Por el contrario, la posición del Comité Internacional de la Cruz Roja (2015), en relación al fenómeno de los grupos armados con un supuesto alcance mundial como Al Qaeda o el DAESH, es que no se considera que se esté desarrollando o se haya desarrollado, un conflicto armado de dimensiones mundiales. Para ello, se requeriría, en primer lugar, la existencia de una parte no estatal "unitaria" en contra de uno o más Estados, lo que no es una realidad.

Sin embargo, no solo resulta indispensable clarificar conceptos que serán utilizados en la investigación, sino que también habría que tener consenso en la investigación con relación al contenido de ciertos principios que serán empleados.

En la presente investigación, las definiciones serán tomadas del Comité Internacional de la Cruz Roja:

a. Principio de humanidad

Se debe tratar con humanidad a todas aquellas personas que no participen en las hostilidades (incluso miembros de las Fuerzas armadas que hayan depuesto las armas y las personas que hayan quedado fuera de combate por enfermedad, herida, detención o cualquier otra causa).

b. Principio de necesidad militar

El DIH establece un delicado equilibrio entre las necesidades de la guerra y los condicionamientos humanitarios, de forma que no se deben causar al adversario males desproporcionados en relación con el objetivo del conflicto armado, que es vencer al enemigo.

Supone optar por el mal menor para no causar a la parte adversa mayor violencia que la exigida por el desarrollo de las hostilidades.

c. Principio de distinción

Las partes en conflicto deben distinguir en todo momento entre la población y los combatientes. Los ataques deben ser dirigidos únicamente contra los combatientes y no contra la población civil. Se hará también distinción entre los bienes civiles y los objetivos militares.

Los ataques no pueden ser dirigidos contra los bienes civiles.

d. Principio de proporcionalidad

Se prohíben las armas y los métodos que causen a las personas civiles y a sus bienes daños excesivos con respecto a la ventaja militar concreta y directa prevista. Así, se prohíbe lanzar ataques cuando sea de prever que causarán incidentalmente muertos y heridos entra la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar prevista.

e. Principio de limitación de la acción hostil

No es ilimitado el derecho de las partes en conflicto a elegir los medios y modos de combatir contra la aparte adversa. De manera que existen medios (armas) lícitos e ilícitos y formas de emplearlos (modos) permitidos o contrarios al DIH.

3. Marco metodológico

Por un lado, es fundamental dejar en claro desde el primer momento que, la presente investigación es meramente teórica, pues a lo largo de ella se

desarrollarán conceptos a partir de datos indirectos, especulativos y no tangibles; por lo que se emplearán métodos de pensamiento lógico.

Con relación al primer punto del esquema de la investigación, es decir, la introducción, se utilizará el método descriptivo, ya que es el único que permite enfocar el objeto de estudio desde un punto de vista amplio, pues lo que se busca a través de ella, es, de manera muy breve, presentar la temática y los principales objetivos del trabajo. Sumado a ello, se tendrá en consideración la importancia del tema.

Respecto a los puntos del esquema que tienen relación con la definición de terrorismo y de ciberterrorismo, el método más adecuado para abordarlos es el de análisis-síntesis, pues es el que posibilita descomponer el objeto de estudio en sus elementos para posteriormente, recomponerlo a partir de la integración de los elementos ya analizados, esta metodología es la más acorde en razón de la problemática para el consenso en la definición de terrorismo y por ende, de ciberterrorismo.

Sumado a ello, el método deductivo será igualmente importante para el caso de la definición de ciberterrorismo, dado que implica sistematizar conocimiento y establecer inferencias. Es decir, permite abordar lo desconocido a partir de lo conocido.

El método descriptivo, también llamado jurídico-descriptivo, será clave para el desarrollo del tercer punto del esquema de trabajo, puesto que el objetivo es dar un panorama de la regulación desde la perspectiva del DIH.

Por otro lado, las herramientas que serán utilizadas para la presente investigación son los análisis doctrinales, los diversos pronunciamientos por parte de Organizaciones Internacionales que tienen relación con la materia y la normativa internacional vinculada al fenómeno terrorista.

4. Desarrollo

En armonía con todo lo antes descrito es menester comenzar el presente apartado con el análisis de lo siguiente:

4.1 Migración del terrorismo al ciberespacio

Es decir, ¿Qué sucede cuando el terrorismo migra a este nuevo escenario? Para responder a la interrogante, es fundamental primero aclarar la realidad en el ciberespacio.

Sobre la materia, Gil Navalón (2012), Jefe de Unidad en el Área de Seguridad de la Información de la Subdirección General de Tecnologías de la Información y Comunicaciones del Ministerio de Defensa español, menciona que algunas de las principales cuestiones relativas al ciberespacio que requieren de definición legal y que confirman el vacío legal de normativa aplicable a la red, son el establecer hasta qué nivel el uso del ciberespacio es un derecho y cómo debe ser protegido, coordinar las acciones legales que, a consecuencia de actos en el ciberespacio, afecten a varias jurisdicciones y acordar las limitaciones al posible uso del ciberespacio en diversos conflictos.

Por lo tanto, es necesario saber qué hacer ante esta nueva realidad virtual caracterizada por la ausencia de fronteras, la dificultad de identificar a los que están actuando con intenciones maliciosas en el ciberespacio y la rápida difusión de las acciones.

En atención a la sensación de incertidumbre, la pregunta lógica es si ¿Es necesario regular las formas de comportamiento en el ciberespacio o, por el contrario, se debe de entender como un “lugar” de libertad absoluta?

Algunos expertos sostienen que el ciberespacio es enormemente regulable y estiman esto necesario, en razón de que el ciberespacio es un escenario

en el que suceden gran cantidad de delitos y existe dificultad para encontrar a los autores, para que respondan de sus hechos (Díaz de Terán, 2013). Los principales argumentos de esta posición son que un espacio de libertad absoluta es una utopía. La realidad es que el ciberespacio es una prueba más que el ser humano no puede vivir en un mundo sin normas, pues sin ellas solo habría descontrol (Díaz de Terán, 2013).

En el extremo opuesto a la necesidad de regulación están aquellos que defienden la libertad absoluta. Perry Barlow así lo afirmó en la Declaración de Independencia del Ciberespacio (1996):

> *Gobiernos del Mundo Industrial (...). No son bienvenidos entre nosotros. No tienen ninguna supremacía donde nos juntamos (…). El Ciberespacio está fuera de sus fronteras. Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o al inconformismo.*

Sus partidarios no consideran que ningún Estado ni Organización deban participar en la regulación, al considerar que el ciberespacio es un espacio de libertad. Es decir, para esta parte de la doctrina cualquier intento de regulación podría catalogarse como censura, pues la libertad de expresión no debe ser condicionada. De la misma manera, no se podría admitir una ordenación efectiva y completa de la red.

Para aquellos que afirmen que la regulación es necesaria, queda plantear una pregunta más: ¿La regulación del ciberespacio se hará desde la autorregulación o desde la heterorregulación? Por un lado, Reguera Sánchez (2015) afirma que la autorregulación hace referencia a una regulación desde el interior de la red por los usuarios de la misma, la que tendría como fundamento la confianza mutua y la responsabilidad

compartida de los usuarios. Aquí se produciría un desplazamiento del ajuste normativo desde los juristas hacia los usuarios y empresas.

Los defensores de la autorregulación lo hacen, principalmente, en base a los problemas que pueden surgir, ante cualquier actividad que sobrepase las fronteras físicas, como el carácter internacional de la red y la dificultad para imponer reglas a los participantes (López, 2006). En la misma línea, Reguera Sánchez (2015) sostiene que la autorregulación presentaría tanto ventajas como desventajas.

Entre las ventajas se encuentran el que el internet surgió como el espacio de máxima libertad, y puesto que hay que elegir entre autorregulación o heterorregulación, parece claro que es la primera la única opción factible en el camino de la normalización. Además, sería más fácil y rápido crear un sistema normativo internacional que no dependiera de fronteras físicas, el que sería válido a nivel mundial.

Entre las desventajas se encuentran el que el orden (la regulación) sería llevado a cabo en base a normas éticas, la exigencia de responsabilidades tendría serias dificultades, pues los actores no son siempre identificables o pueden encontrarse fuera de alcance. También se dejaría la labor de impartir justicia y aplicar sanciones en los propios usuarios de la red. En adición a ello, la regulación por parte de la red, carecería de legitimidad democrática.

Así, Suñé Llinás señala que la libertad pasa por la intervención mínima del poder, lo que supone la necesidad de dejar amplios espacios abiertos a la autorregulación; pero siempre dentro de un marco legal que sea verdaderamente un orden de libertad (2009).

Por otro lado, hay quienes consideran que la mejor forma de regular el ciberespacio es la heterorregulación, la que, según Reguera Sánchez (2015), se define como una regulación desde fuera de los usuarios; que puede ser regulada ya sea por el legislador nacional, bien sea por acuerdos internacionales o por parte de acuerdos entre Estados y Organizaciones Internacionales. Esta posición se sustenta en que los gobiernos tienen la obligación de proteger los derechos fundamentales de sus ciudadanos en cualquier dimensión en la que actúen, tanto en tierra, mar, aire y por qué no, en el ciberespacio.

Los motivos que hacen que la doctrina se decante por la heterorregulación son que según López Zamora (2006) una sociedad autorregulada no es posible, pues eso sería una utopía y, de la misma manera, tampoco lo puede ser el ciberespacio. Así, es claro que la única solución es que el Derecho, a través de sus instituciones, entre en la cibersociedad.

Pero, a las ventajas antes señaladas hay que sumar las desventajas, como que en el ciberespacio conviven diferentes tipos de redes, usuarios de diferentes costumbres, éticas y moral. Es por esta razón que los acuerdos en las normas se deben alcanzar desde el consenso internacional (Reguera, 2015).

La realidad, al igual que la presente investigación, ha optado por la heterorregulación y es en esa línea que la OTAN durante la conferencia de Praga de 2002 decidió poner en marcha un programa global de coordinación de la ciberdefensa, con el objetivo de luchar contra los ataques informáticos. No fue hasta después de los acontecimientos ocurridos en abril del 2007 en Estonia, que se decidió trabajar para definir un nuevo concepto estratégico de ciberdefensa, el cual tomo forma en la Cumbre de Lisboa en el año 2010.

En cuanto a Naciones Unidas, las iniciativas para regular y buscar un consenso han sido escasas, pero se pueden señalar como principales resoluciones en esta área:

- Resolución de la Asamblea General 55/63 (2000) y 56/121 (2001), a través de las cuales se invita a los Estados Miembros a que tomen en cuenta las medidas propuestas al elaborar leyes y políticas nacionales, para combatir la utilización de la tecnología de la información con fines delictivos.

- Resolución de la Asamblea General 57/239 (2002) para la creación de una cultura global de ciberseguridad, en la que se exhorta a tener en cuenta los principios de: conciencia, responsabilidad, respuesta ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación.

- Resolución de la Asamblea General 58/199 (2004) para la protección de las infraestructuras de información, en la que se busca estimular el desarrollo de normas de conducta en el ciberespacio.

En relación al Consejo de Europa, esta ha sido la primera organización internacional en adoptar un tratado para la lucha contra los delitos en internet, el Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest), el que entró en vigencia en julio de 2004.

Ahora bien, con relación al caso de la Unión Europea, en mayo de 2010 la Comisión Europea presentó una comunicación titulada una Agenda Digital para Europa, la que constituye uno de los siete pilares de la Estrategia Europea 2020.

Teniendo en cuenta este panorama es ahora necesario centrarnos en lo medular de la investigación: el ciberterrorismo; sin embargo, no podemos

dejar de hacer referencia a los ciberataques, los que pueden ser definidos como las operaciones cibernéticas ofensivas o defensivas de las que se espera que puedan causar pérdidas de vidas humanas, lesiones a las personas y daños o destrucciones de bienes (Barat-Ginies, 2013).

Desde la aparición de los ciberataques las naciones y organizaciones han ido reaccionando de forma progresiva para enfrentarse contra esta amenaza global sin precedentes. De esta forma, se han creado sistemas de respuesta y diferentes estrategias para garantizar la seguridad de sus ciudadanos y empresas. Es en ese sentido que, en el ámbito jurídico internacional, siguiendo el *ius ad bellum* de la Carta de las Naciones Unidas (ONU), este tipo de ataques cibernéticos de un Estado contra otro, tienen la siguiente consideración según Pons Gamón (2017):

> *"Podrían ser considerados como "uso de la fuerza" y pueden provocar un conflicto armado internacional; el Estado atacado tendría derecho a defenderse legítimamente mediante un ataque armado, de forma general el Consejo de Seguridad considera estos actos como de agresión y amenaza a la paz, por lo que podría intervenir para restablecer la paz y la seguridad internacional"*

En la misma línea, Carlini (2016, p. 8) indica que "para entender mejor los ataques cibernéticos como uso de la fuerza tendría que tenerse en consideración el instrumento, el objeto y un enfoque basado en los efectos". Igualmente el trabajo realizado por el Grupo de Expertos del Centro de Excelencia de la OTAN para la Ciberdefensa de Tallín, menciona que el derecho internacional vigente es de aplicación a las operaciones cibernéticas y los Estados podrán ejercer el derecho de la legítima defensa (CCDCOE, 2013).

Ahora bien, el terrorismo internacional tiene una lógica distinta de respuesta, pues no estamos ante un conflicto entre estados, sino que el perpetrador es un grupo terrorista, entre los que el yihadista se ha caracterizado por ser el que más ha empleado la red para la divulgación de sus ideas y sus métodos de ataques, así han incorporado nuevas formas de agresión, sobre todo orientadas a la captación, adiestramiento o adoctrinamiento en el odio, del que no tendrán reparos en emplear de manera cruel contra sus enemigos (Pons, 2017).

4.2 Nuevo escenario de confrontación

En línea de todo lo antes expuesto, es evidente que nos encontramos ante un escenario nuevo de confrontación con el terrorismo, el mismo que ha sido explicado en el apartado 4 a detalle, llegando a la conclusión que no existe un consenso sobre el concepto. Por ello, de manera muy breve, partiendo de diversas características alegadas por la doctrina al fenómeno, se acuñara un propia.

Alex Schmid (2012), afirma que una correcta definición de terrorismo debe describir varios puntos, siendo los principales: el hacer referencia al contexto en el que el terrorismo se emplea, incluir el concepto de violencia física o amenaza de la misma y mencionar que el terrorismo produce miedo, pánico, ansiedad, etc.

Sumado a ello, Lutz y Lutz (2013) presentan una definición propia en donde el terrorismo implica seis puntos:

> *"(1) El terrorismo involucra el uso de violencia o amenazas de violencia (2) por parte de un grupo organizado (3) para lograr objetivos políticos. La violencia (4) está dirigida contra una audiencia objetivo que se extiende más allá de las víctimas inmediatas, que a menudo son civiles inocentes. Además (5), aunque un gobierno puede ser el perpetrador de la violencia*

o el objetivo, se considera un acto de terrorismo sólo si uno o ambos actores no son un gobierno. Finalmente, (6) el terrorismo es un arma de los débiles"

En ese sentido y tomando en cuenta lo anterior, podemos definir al acto terrorista como cualquier práctica de violencia o amenaza de ella llevada a cabo por un individuo o grupo ajeno al gobierno, con la finalidad de producir daño y/o un estado psicológico de terror con el objetivo de captar adeptos y/o alcanzar sus demandas.

En esa línea, diferencia del terrorismo, el ciberterrorismo como ya ha sido evidenciado, no cuenta con una realidad medible y cuantificable; por ello Ibañez (2014) afirmó años atrás que la mayoría de los incidentes, en el ciberespacio, que se han producido ni han sido lanzados por grupos terroristas contra infraestructuras críticas o a gran escala, ni han tenido consecuencias graves y duraderas que se conozcan.

Así, se pueden brindar ciertos ejemplos de ciberataques, entre los que se encuentran:

"Aunque raros, los ciberataques destructivos originados por el Estado se han convertido en un instrumento de poder nacional.

Los ejemplos incluyen Stuxnet, el presunto ataque estadounidense-israelí contra el programa nuclear iraní; la explotación china de redes en todo el mundo; rusos derribando redes en Estonia, Georgia y Ucrania; ataques norcoreanos contra sistemas comerciales en Corea del Sur y Estados Unidos, y ataques iraníes contra instituciones financieras estadounidenses y sobre el sector energético saudita". (Dobbins, 2015)

Sin embargo, en estos casos al ser el perpetrador el Estado, los ejemplos no se ajustan a la definición de terrorismo planteada por la presente investigación. Entonces, podrían existir posiciones, válidas, que sostuvieran "Si no ha habido un ataque "importante" desde el ciberterrorismo ¿Por qué darle atención?"

Weimann (2007) responde a la pregunta señalando que debido a que la mayoría de las infraestructuras críticas en las sociedades se conectan en la red a través de las computadoras, la amenaza potencial del ciberterrorismo es, sin duda, muy alarmante.

4.3 Panorama normativo del DIH y su relación con el fenómeno terrorista

Ya que comprendemos la complejidad del ciberespacio y hemos limitado los contornos de una definición amplia de terrorismo es momento de brindar el panorama normativo correspondiente al DIH. Para ello, lo primero es acercarnos a la materia ¿Qué es?

El DIH, según menciona Salmón (2004) es aquel que no permite ni prohíbe los conflictos armados, tanto internacionales como internos, sino que, frente a su desencadenamiento, se aboca al fin de humanizarlos y limitar sus efectos a lo estrictamente necesario (p.23).

Sin embargo, y resulta una pregunta válida, podría uno cuestionarse ¿Qué tiene que ver un conflicto armado con el terrorismo? ¿Cúal es la relación entre el DIH y el terrorismo? Para poder responder a la interrogante es imprescindible contextualizar el tema.

Sobre la materia, el Comité Internacional de la Cruz Roja (en adelante, CICR) menciona que, como consecuencia inmediata de los ataques de septiembre 11 de 2001 contra los Estados Unidos se dió inicio a lo que se ha denominado "guerra contra el terrorismo" (2003, p. 19). Pero, ¿estamos ante una guerra en un sentido jurídico?

De acuerdo a lo mencionado por el CICR, quienes sostienen que se está librando esencialmente una guerra en el sentido jurídico están convencidos de que lo ocurrido en septiembre 11 y los acontecimientos siguientes a el confirman el surgimiento de un nuevo fenómeno, uno que tiene intima relación con redes transnacionales con capacidad de infligir violencia mortífera en Estados geográficamente distantes. Sumado a ello, se afirma que respecto a la índole transnacional, esta queda demostrada por el hecho de que sus actividades no son por lo general imputables a un Estado específico en virtud de las reglas sobre la responsabilidad de los Estados (2003, p. 19).

En ese sentido, una respuesta desde la represión del delito resulta inadecuada e incluso, desfasada, ya que al tomar en cuenta no solo la magnitud, sino también el potencial detrás de los ataques terroristas, estos se acercan a la categoría de actos de guerra, no a la clásica definición de delito. Es decir, la posición de una parte de la doctrina es que, ya que el mundo se enfrenta a un nuevo tipo de violencia, como ha quedado evidenciado, a este se le deberían aplicar las reglas del conflicto armado; esto aún cuando no se ajusta a las definiciones clásicas de CAI y CANI.

No obstante, existe otra parte de la doctrina que considera que el terrorismo no es un fenómeno nuevo; sino que por el contrario, durante años se han llevado a cabo actos de terrorismo, los mismos que han dado lugar a una serie de convenios internacionales que los penalizan y obligan a los Estados a cooperar en su prevención.

Aunado a ello, el que las personas o grupos de ellas puedan dirigir su violencia traspasando fronteras internacionales o creando redes transnacionales no justifica, en sí mismo, el calificar este fenómeno como conflicto armado (CICR, 2003, p. 19).

Lo cierto es que, sin importar lo que la doctrina sostenga, el CICR en el Informe Ejecutivo preparado con ocasión de la conferencia sobre el derecho internacional humanitario y los retos de los conflictos armados contemporáneos ha afirmado públicamente que considera que el derecho internacional humanitario es aplicable cuando la “lucha contra el terrorismo” equivale o implica un conflicto armado, (2003, p. 21), afirmación que si bien resulta útil no termina de aclarar nuestras dudas.

Y es que, para el CICR no hay certeza acerca de si la totalidad de la violencia que ocurre entre Estados y redes transnacionales pueda considerarse conflicto armado en el sentido jurídico; ya que resulta complejo que una red clandestina de células sin mucha conexión, reuna las condiciones para ser considerada “parte” en el conflicto.

En línea de lo mencionado, resulta imprescindible recordar que el DIH sólo es aplicable en conflictos armados, siendo uno de los elementos fundamentales la existencia de "partes" en el conflicto, concepto que sera desarollado más adelante.

En consecuencia, el CICR termina concluyendo que son muchas manifestaciones de violencia que actualmente se producen en diversas partes del mundo y que suelen ser calificadas de "terroristas", sin embargo, son perpetradas por grupos poco organizados (redes) o por individuos que, en el mejor de los casos, tienen una ideología común. Por lo tanto, con las pruebas de que habitualmente se dispone, no es posible calificar a esos grupos o redes como partes de algún tipo de conflicto armado, ni siquiera de un conflicto "transnacional" (2003).

Pero, ¿Qué sucede si el grupo terrorista si cuenta con organización y con una estructura de mando? ¿Inmediantamente podríamos afirmar el CAI o CANI?. Para dar respuesta, es menester remitirnos a la normativa pertinente.

El DIH se encuentra principalmente contenido en los cuatro Convenios de Ginebra de 1949, más sus dos Protocolos Adicionales de 1977, relativos a la protección de las víctimas de los conflictos armados: el Protocolo I para conflictos armados internacionales y el Protocolo II para conflictos armados no internacionales.

Así, es importante distinguir los conflictos armados en internacionales (CAI) y no internacionales (CANI), pues según su tipo varían las normas aplicables, siendo bastante más extensiva la aplicación de las normas para el primer supuesto. Esto último debido a la reticencia que tienen ciertos Estados a someterse a reglas internacionales que indiquen cómo han de comportarse frente a un conflicto armado interno suscitado entre grupos armados no estatales entre sí o contra las fuerzas armadas de su propio Estado (Gutiérrez, 2014).

De otro lado, al mencionar a los CANI, estos están básicamente sujetos al Derecho establecido en el artículo 3° común de los Convenios de Ginebra, más el Segundo Protocolo Adicional.

Introducido el tema, existen dos maneras de encuadrar un supuesto acto terrorista dentro de la órbita jurídica del DIH; o lo clasificamos como un CAI o como un CANI. ¿Cómo hacerlo? Determinando la existencia de un conflicto armado.

Los jueces del Tribunal Penal Internacional para la ex-Yugoslavia en el fallo Tadic, del 2 de octubre de 1995, brindaron de manera general los elementos necesarios para hablar de un conflicto armado:

> *Un conflicto armado existe toda vez que se emplea el uso de la fuerza armada entre Estados (CAI) o cuando existe un conflicto armado prolongado entre autoridades gubernamentales y grupos armados organizados o entre estos mismos grupos en el seno de un Estado (CANI).*

Este mismo tribunal especifica con relación a los CAI que estos existen toda vez que hay un uso de la fuerza armada entre Estados; definición que se encuentra en armonía con el artículo 2° común de los Convenios.

En ese sentido, aunque con evidentes rasgos actuales de lo que consideramos "conflictos hibridos", para Jéremie Swinnen (2018), los CAI pueden ser de tres tipos:

1) Los conflictos armados interestatales.

2) Los CANI que se internacionalizan por la intervención de un Estado o una organización internacional.

3) Guerras de liberación nacional.

Por otro lado, con respecto al ámbito de aplicación material de los CANI, el autor antes mencionado sostiene que no cualquier ataque puede ser calificado como conflicto armado y ser regido por el DIH, pues para recaer en el ámbito de un conflicto armado no internacional, la jurisprudencia internacional, en especial el Tribunal Internacional para la Antigua Yugoslavia, ha recurrido principalmente a dos criterios:

i) Un mínimo de intensidad en el conflicto

ii) Organización de las partes involucradas

Además, para terminar de entender el porqué de los criterios, resulta fundamental remitirnos al artículo 1° del Segundo Protocolo Adicional, pues en el se indica que no será de aplicación la norma para:

las situaciones de tensiones internas y de disturbios interiores, tales como los motines, los actos esporádicos y aislados de violencia y otros actos análogos, que no son conflictos armados.

Es decir, el alcance jurídico de los Convenios de Ginebra y los Protocolos para el CANI requiere que el acto revista de suficiente intensidad; lo que como resulta evidente tiene relación con un nivel de organización. En consecuencia, podemos afirmar sin temor a equivocación que si de una evaluación del caso por caso, se concluye que las partes cuentan con una importante estructura organizativa y si los ataques alcanzan el nivel de intensidad requerido, el que puede medirse según el CICR (2012) por número de combatientes, tipo de armas, número de víctimas, planificar operaciones, reclutamiento, etc; estaremos ante un CANI y por ende, sería de aplicación el DIH.

Distinto es para los CAI, ya que los mismos se constituyen independientemente de la intensidad, pues es suficiente con que un Estado intervenga aún indirectamente para internacionalizar el conflicto (Swinnen, 2018). ¿Qué significa esto? Para el autor, en la medida en que se pueda conectar un acto terrorista con la intervención de otro Estado, este acto podrá enmarcarse dentro de los límites del DIH. Pero, ¿Cómo conectarlo? Swinnen lo clarifica de la siguiente forma:

> *Existen tres grandes posibilidades de relacionar un determinado grupo armado o la comisión de un acto terrorista con el accionar de un Estado. Ello, principalmente, a través de un examen de responsabilidad internacional.*
>
> *1. Cuando un grupo armado está habilitado por el derecho de un Estado a ejercer prerrogativas de poder público o cuando el mismo constituya de facto el gobierno de ese mismo Estado. (La guerra librada por Estados Unidos contra Afganistán hasta junio de 2002 es un ejemplo; territorio en el cual los talibanes ejercían un poder efectivo en gran parte del territorio).*
>
> *2. Cuando un grupo armado actúa bajo el control o la dirección de otro Estado.*

3. Cuando un Estado adopta como suyo un determinado comportamiento o actos. (Ejemplo ocurrido en la toma de rehenes en la embajada norteamericana en Teherán).

Ahora bien, a sabiendas que un acto de terrorismo sí puede ser analizado desde el DIH, respondamos a las siguientes preguntas: ¿Qué entiende el DIH por actos de terrorismo? ¿Qué dicen los Convenios de Ginebra y sus dos Protocolos Adicionales al respecto?

El DIH posee cuatro referencias relacionadas con el terrorismo. Dos artículos para los CAI y dos artículos para los CANI. Con relación a los primeros se sostiene:

- Artículo 33° del IV Convenio.-

  Están prohibidos los castigos colectivos, así como toda medida de intimidación o de terrorismo.

- Artículo 51° del Primer Protocolo Adicional.-

  Quedan prohibido los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil.

De otro lado, con relación a los conflictos armados no internacionales, los artículos pertienentes son:

- Artículo 13° del Segundo Protocolo Adicional.-

  Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil.

- Artículo 4° del Segundo Protocolo Adicional

  […] están y quedarán prohibidos en todo tiempo y lugar […] los actos de terrorismo […].

Los artículos hacen referencia a conceptos como “actos de terrorismo”, “terrorismo” y “aterrorizar”, pero ¿Cómo se definen? Tal y como ya ha sido analizado, estos conceptos no tienen una definición consensuada, por esa razón, el presente artículo, ha tenido como objetivo brindar una para entender al acto terrorista, recordemos:

> *cualquier práctica de violencia o amenaza de ella llevada a cabo por un individuo o grupo ajeno al gobierno, con la finalidad de producir daño y/o un estado psicológico de terror con el objetivo de captar adeptos y/o alcanzar sus demandas.*

No obstante, para poder interpretarla de forma correcta es menester entender que el DIH exige la contemplación de principios como por ejemplo el de necesidad militar, el que prevé que ciertos actos bélicos estén permitidos, incluso si ellos pueden generar terror. ¿Entonces? Nuestra definición necesita una mayor precisión:

> *práctica de violencia o amenaza de ella llevada a cabo por un individuo o grupo ajeno al gobierno, con la finalidad de producir daño y/o un estado psicológico de terror <u>a población civil</u> con el objetivo de captar adeptos y/o alcanzar sus demandas.*

Esa precisión permite asegurar que nuestra definición se encuentre en armonía con lo expresado por el Consejo de Estado Colombiano en su fallo de 2015, pues no todos los actos de terror son penados por el DIH, por el contrario, los actos de terror pueden considerarse permitidos, desde un punto de vista jurídico, si es que se dirige exclusivamente contra quienes participan directamente en las hostilidades y siempre que se cumplan los principios del DIH.

En ese mismo sentido se ha pronunciado la doctrina, expresando que la realidad es que el terror también es un arma que puede ser utilizada contra las fuerzas armadas de la parte adversa (Gasser, 2002).

Ya que conocemos las características necesarias para habilitar la protección del DIH ante un acto terrorista, es momento de centrarnos en el DAESH.

4.4. Conociendo al DAESH

En palabras de Eugenia López- Jacoíste (2018) uno de los grupos rebeldes más radicales opositores al régimen de Damasco es el autodenominado Estado Islámico que a partir del 2014 ha sitiado y ocupado por la fuerza ciudades importantes de Siria como Homs, Allepo y Raqqa o Mosul en Irak mediante asesinatos colectivos, amenazas y abusos a las poblaciones con el fin de proclamar su califato (p. 226).

Si bien no es posible por la extensión del presente trabajo, detallar la historia detrás del surgimiento del DAESH, lo que queda claro es que en Siria existe una de las mayores y más complejas crisis humanitarias, cifras del CICR al 2017 sostuvieron:

- 6, 5 millones de desplazados internos
- 5 millones de personas viven en ciudades sitiadas y/o en zonas de dificil acceso, lo que tiene intima relación con la falta de suministros básicos
- 5 millones de refugiados se encuentran en países cercanos como Líbano, Jordania e Irak.

Pero, ¿Cómo se llegó a esas cifras? El actual conflicto armado contra el DAESH que se extiende por territorio iraquí y sirio es consecuencia de dos grandes factores para López- Jacoíste: por un lado, la evolución de las revueltas de la primavera árabe en Siria y por otro lado, la frágil situación iraquí posterior al 2011, consecuencia de la retira de tropas norteamericanas del territorio. Sumado a ello, la autora menciona que no hay que olvidar los factores económicos y religiosos, y, el elevado número

de Estados que de forma progresiva se han incorporado a la coalición internacional en apoyo a Irak y Siria.

Hemos hablado de Siria e Irak como los grandes oponentes del DAESH, pero ¿Cómo calificar esos conflictos? ¿Es un CAI, porque se autodenominan Estado? ¿Actúan bajo control de otro Estado?, o, ¿Es un CANI? ¿Cuenta con una estructura suficiente de organización?

Eugenia López (2018, p. 241) es clara al afirmar que los conflictos armados contra el DAESH, tanto el de Siria como el de Irak, no son conflictos armados internacionales, porque a pesar de su normbre, el Estado Islámico no es un Estado según el Derecho Internacional. Si bien detallar las razones por las que efectivamente no es un Estado resulta clave, al no ser el principal objetivo de la investigación, solo se aludira a lo mencionado por Sánchez Naranjo (2019):

> *[…] que, aunque el Estado Islámico cumpla de hecho los requisitos enunciados en la fuente de derecho internacional mencionada […], es conveniente recordar que existen ciertos vicios invalidantes en la creación de un Estado que impiden tener al Estado Islámico esa denominación en el derecho internacional.*
>
> *Estos elementos que se consideran inválidos son el territorio y la población.*
>
> *Por un lado, el del territorio no se cumple al haberse producido dicha adquisición territorial contraviniendo normas imperativas de derecho internacional general. Similar apreciación se hace acerca del incumplimiento del elemento poblacional, al haber existido múltiples violaciones de derecho internacional humanitario habiendo empleado medios como las armas químicas o incluso la utilización de la tortura contra los oriundos.*

En este caso, resultaría aplicable el proverbio latino "ex injura ius non oritur". Por consiguiente, el concepto más preciso o ajustado para definir a esta realidad que es el Estado Islámico es la de grupo terrorista.

Aunado a lo anterior, tampoco podemos afirmar que el DAESH es un actor no estatal que actúa bajo el control global de otro Estado, ya que para ello, en armonía con el Tribunal Penal Internacional para la Ex-Yugoslavia en el caso Tadic en Sala de Apelaciones y la Corte Internacional de Justicia en el caso de Nicaragua (1986), el criterio de control se cumple en la medida que un Estado Extranjero desempeña un papel en la organización, coordinación y planificación de las acciones militares, además de financiar, instruir y equiparar o prestar apoyo en las operaciones. En palabras simples, para afirmar que actúa bajo el control de otro Estado, el DAESH tendría que cumplir órdenes, estar bajo el mando o control de real de por ejemplo, Arabia Saudí; lo que no resulta acorde con la realidad.

Al descartar la calificación de CAI, pasemos al análisis del CANI, el primer artículo que merece nuestra atención es el 3° común ¿Qué se exige? Por un lado, que estemos ante un conflicto armado, es decir que exista violencia armada (acción hostil) de carácter colectivo, y que exista un mínimo de organización, es decir, en términos sencillos, hablamos de organización e intensidad, como se indico párrafos arriba.

Ahora, con relación a la organización, en el Informe (2011) sobre Derecho Internacional Humanitario y los desafíos de los conflictos armados internacional de la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja se sostiene que entre los elementos indicativos que sirven de base para considerar este criterios, estos incluyen:

- *la existencia de una estructura de mando*
- *la existencia de normas y mecanismos de disciplina dentro del grupo armado*

- *un centro de operaciones, la capacidad de procurarse, transportar y distribuir armas*
- *la capacidad del grupo de planificar, coordinar y llevar a cabo operaciones militares, incluidos los movimientos de las tropas y la logística*
- *capacidad para negociar y pactar acuerdos, por ejemplo un alto el fuego o un acuerdo de paz.*

Dicho de otra manera, a pesar de que el nivel de violencia en una situación concreta puede ser muy alto, para hablar de CANI es necesaria la organización. ¿Esto se cumple en el DAESH? López-Jacoíste (2018) explica la situación haciendo énfasis en que una vez que se desmarcó de Al Qaeda y Al Nursa a finales de 2012, el DAESH inicio su campaña militar para la adquisición de territorio a lo largo del 2014 hasta llegar a controlar grandes extensiones que iban desde Mosul a Raqqa, siendo la caída de Palmira en mayo del 2015 su última gran conquista. En ese mismo año, comenzó a perder ciudades clave en Irak, asi como en el norte de Siria (p. 247).

No obstante, eso no aminoro su poder en realidad, prueba de ello es que en el año 2015 a través de la Resolución 2249, el Consejo de Seguridad exhorto a los Estados Miembros a adoptar medidas sobre el territorio bajo el control del DAESH, acordes con el DIH, para prevenir y reprimir los actos terroristas cometidos.

Lo mencionado muestra una organización suficiente que le ha permitido hacerse y mantener el control territorial en ciudades clave.

En el mismo informe antes citado, también se toca el tema de la intensidad y con relación a ella se indica que es un criterio fáctico, cuya evaluación depende de un examen de lo que ocurre sobre el terreno. No obstante, entre los elementos indicativos para la evaluación se incluyen:

- *el número de enfrentamientos y la duración e intensidad de cada uno de ellos*
- *el tipo de armas y de otros material militar utilizado, el número y el calibre de las municiones utilizadas, el número de personas y los tipos de fuerzas que participan en los enfrentamientos*
- *el número de bajas, la extensión de la destrucción material y el número de civiles que huyen de las zonas de combate.*

Sumado a ello, el Tribunal Penal Internacional para ex Yugoslavia (TPIY), sostiene que existe un CANI en el sentido del artículo 3° común cuando hay una violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados.

¿Qué sucede con el DAESH? La Comisión Internacional Independiente de Investigación sobre la República Árabe Siria (2014) ha confirmado el múltiples informes el uso de cloro gaseoso así como otras armas prohibidas como las bombas barril. Aunado a ello, la Comisión ha tomado conocimiento de crímenes de guerra, torturas y tratos crueles, al igual que asesinatos, ejecuciones extrajudiciales, toma de rehenes, desapariciones forzadas, lapidaciones, actos de violencia sexual, decapitaciones, etc.

Por lo que es posible afirmar que con relación a estos conflictos en particular la existencia de un CANI.

Sin embargo, y aunque lo anterior es ejemplificativo, no responde a la pregunta vertebral de la investigación, la que tiene que ver con:

4.5. Los ataques de ciberterrorismo perpetrados por el DAESH

Aquí las interrogantes se vuelven más complejas ¿Qué tan “ciber” es el DAESH? ¿Sólo hablaremos de las decapitaciones televisadas? ¿Qué sucede con la gran cantidad de propaganda con la que cuentan?

Lo primero que hay que tener en consideración es que la estrategia mediática del DAESH ha sido ampliamente estudiada en sectores académicos, los mismos concluyen que su propaganda se basa en imágenes de alto impacto y cuidados rodajes y ediciones audiovisuales. Aunado al uso no sólo de la web sino también de las redes sociales (Cano Paños, 2019). Y es que de lo que conocemos y hasta ahora ha sido desarrollado en el texto, es evidente que la propaganda se ha convertido en una de sus principales armas, para 2 fines en particular: reclutar a nuevos seguidores, y para sembrar el terror.

Según Gaviña (2017) parte de lo que caracteriza al primer fin incluye revistas, como la oficial *«Dabiq»;* emisoras de radio, como *«La voz del Califato»,* en Nangarhar, Afganistán, y de televisión, como *BEIN HD4;* con el objetivo de que su interpretación radical del islam llegue al mayor número posible de personas, pero especilamente de los más jóvenes.

En línea de lo mencionado, la autora brinda cifras (2017) siendo que desde enero de 2014 hasta el 2017, DAESH ha distribuido, a través de redes sociales como Facebook, Twitter y YouTube, más de un millar de vídeos en los que se ven asesinatos y se reivindican atentados. No obstante, no todos los contenidos hablan de violencia, solo cerca del 15%.

Gaviña sostiene que en tanto el perfil de la audiencia que persiguen es el de jóvenes entre los 15 y los 20 años; el contenido de los vídeos busca imitar la estética de producciones cinematográficas de Hollywood. Esto les ha llevado a copiar de manera exacta escenas de películas y series como “Saw” o “Matrix” (2017).

¿Qué hacer con ellos? De acuerdo a nuestra definición de terrorismo, algunas muertes por necesidad militar no serían más que daño colateral.

Pero, ¿la idea se mantiene si se decapita rehenes cual ganado en televisión o si se ataca con acido? Es evidente que eso sobrepasa la necesidad militar, es tortura y vejación en su máxima expresión, lo que vulnera las normas de DIH siendo una de ellas, la regla 90 de derecho consuetudinario, la prohibición de la tortura, de los tratos crueles o inhumanos o los atentados contra la dignidad de la persona, en especial los tratos humillantes y degradantes.

Por lo tanto, estos vídeos aún cuando el terror se viralice en la red, se encuentran penados por el DIH, pues calzan dentro de un esquema de conflicto armado tal y como se ha mencionado; y, vulneran las disposiciones más importante de la normativa pertinente.

De otro lado, y no podemos perder de vista que también se utiliza la propaganda para atraer jóvenes “a la causa”, a los que se les muestra los beneficios del Califato, lo que genera un reto, ¿Cómo se pueden neutralizar estos mensajes? ¿Cómo evitar que existan más adeptos? Esas preguntas son importantisimas, y espero sean parte de reflexión de profesionales de la comunicación y la psicología, ya que en la temática no hay discusión con relación al DIH.

5. Conclusiones

Los conflictos han tenido lugar en el mundo desde la existencia misma del ser humano, y es que desde su génesis el hombre ha tenido que enfrentar de una forma cuasi camaleónica las dificultades propias de su época, desde problemas de distribución de animales y posteriormente, de granos hasta lo ampliamente desarollado en la investigación: los conflictos en el ciberespacio, y es que el uso masivo de tecnologías y sistemas de información han permeado cada uno de los aspectos de nuestra vida, desde lo más simple como colocar nuestro Curriculum Vitae en una red social esperando que nuestro entorno profesional nos tome en cuenta,

hasta lo más complejo como lo es vernos expuestos a videos de tortura por parte de un grupo terrorista, con la única finalidad de aterrorizarnos.

Esto último es lo que ha generado las interrogantes que han motivado el presente trabajo de investigación, y es que todos nosotros de una u otra manera, con mayor o menor detalle, hemos escuchado sobre el DAESH y su brutalidad, sabemos de decapitaciones y ácido, pero ¿Qué hacer? ¿Qué nos exige la realidad del ciberterrosimo? Y lo más importante ¿El DIH tiene una respuesta? Lo primero es entender a que nos enfrentamos y para ello estamos obligados a conocer que es o como se configura un acto terrorista; ante la falta de consenso sobre la definición del mismo en la doctrina y ante la ausencia de posición en la normativa, consideramos oportuno brindar una definición propia.

Lo siguiente a responder es si estos actos, contrarios al DIH, se configuran también en el uso de armas propagadoras del terror como lo son los vídeos del DAESH y según lo analizado es válido el uso de las normas del DIH para regular los conflictos surgidos en el ciberespacio. En esa línea, las consecuencias causadas por un ataque cibernético avalan su aplicabilidad siempre que estemos ante un grupo armado organizado, y se confirme que sus acciones cumplen con requisitos de intensidad.

En consecuencia, al preguntarnos si ¿Los ataques de ciberterrorismo perpetrados por el DAESH se encuentran previstos en la definición de terrorismo y por ende, encuentran regulación en el DIH? La respuesta es sí.

Sin embargo, aún hay mucho sobre lo que necesitamos reflexionar; es que, si bien parece que nos hemos adecuado todos a la realidad del ciberespacio, aún nos queda mucho camino por recorrer. ¿Es necesaria una regulación específica para los actos en el ciberespacio en el DIH?

¿Es suficiente la interpretación extensiva? O, en realidad, al ser el escenario distinto, lo más recomendable es repensar la normativa.

Otro tema de suma importancia que nos obliga a pensar es la falta de consenso sobre una definición de terrorismo, la misma que ha llevado a la doctrina a suplir esa deficiencia, muchas veces con incongruencias, aunque también muchas con aciertos. ¿Deberíamos tener una sola definición desde la normativa? O ¿Una definición estática podría generar mayores inconvenientes?

Por otro lado, resulta evidente que las muestras de terror por parte del DAESH sí se dan desde el contexto de un conflicto armado, incluso podemos afirmar que, aunque se viralice en el mundo, el DIH se aplica. ¿Cómo se aplica? ¿Cómo aseguramos la efectividad?

Finalmente, lo más importante de la presente investigación es brindar un panorama que, aunque algunas de sus respuestas generen más dudas que certeza s, obligue a un estudio más profundo de la materia desde la academia.

6. Bibliografía

- Aguirre, J. (2004). Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. *Espéculo: Revista de Estudios Literarios*,*(*27).Recuperado de:https://dialnet.unirioja.es/servlet/articulo?codigo=926974&orden=19934&info=link.

- Barat-Ginies, O. (2013). Informe jurídico del CCD CoE-El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra-Informe final a 22 de noviembre de 2012. Madrid.

- Cano, M. (2019). La expansión, intensificación y seducción del terrorismo islamista a través de internet: análisis criminológico. *Revista Científica General José María Córdova*, *17*(26).

- Carlini, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. Documento de Opinión 67/2016 en Instituto Español de Estudios Estratégicos. Recuperado de:http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO672016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf.

- Casar, J. (2012). Introducción. Monografía del CESEDEN 126 del Centro Superior de Estudios de la Defensa Nacional del Ministerio de Defensa, *El Ciberespacio. Nuevo escenario de confrontación,* 9-35.

- Cebada, A. (2017). Las respuestas de la comunidad internacional a los conflictos internacionales contemporáneos: el caso de Siria. Cuaderno de defensa 188 en Instituto Español de Estudios Estratégicos, *Seguridad Global y derechos fundamentales*, 223- 248.

- Chicharro, A. (2009). La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas. *Revista de Internet, Derecho y Política,* (9), 1-14. Recuperado de: http://www.redalyc.org/ articulo.oa?id=78813254002.

- Chicharro, A. (2013). La violencia terrorista en el ciberespacio: Riesgos y normativa europea sobre ciberterrorismo. En J. Herrero et al, *La Sociedad Ruido/ Entre el dato y el grito* (pp. 80-81). La Laguna, Tenerife: Sociedad Latina de Comunicación Social. Recuperado de: http://www.revistalatinacs .org/068/cuadernos/cac53.pdf.

- Cockburn, P. (16 de febrero de 2019). Trump afirma que el Daesh está derrotado, pero ignora una realidad mucho mayor y más inquietante. *Sin Permiso.* Recuperado de: https://www.sinpermiso.info/textos/trump-afirma-que-el-daesh-esta-derrotado-pero-ignora-una-realidad-mucho-mayor-y-mas-inquietante

- Conway, M. (2006). Terrorism and the Internet: New Media–New Threat?. *Parliamentary Affairs 59* (2), 283-298.

- Comisión Internacional Independiente de Investigación sobre la República Árabe Siria. (2014). A/HRC/27/60 y A/HRC/26/CRP.2

- Comité Internacional de la Cruz Roja. (2003). *El derecho internacional humanitario y los retos de los conflictos armados contemporáneos.*

- Comité Internacional de la Cruz Roja. (2008). *¿Cuál es la definición de "conflicto armado" según el derecho internacional humanitario?.* Recuperado de: https://www.icrc.org/spa/assets/files/other/opinion-paper-armed-conflict-es.pdf.

- Comité Internacional de la Cruz Roja. (2012). *Conflit interne ou autres situations de violence : quelle différence pour les victimes?.* Recuperado de: https://www.icrc.org/fre/resources/documents/interview/2012/12-05-

niac-non-international-armed-conflict.htm. Consultado el 23 de diciembre de 2017).

- Comité Internacional de la Cruz Roja. (2015). XXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos. Informe preparado por el Comité Internacional de la Cruz Roja. Recuperado de: http://rcrcconference.org/wp-content/uploads/2015/10/IC32_Migration-report-ES.pdf.

- Comité Internacional de la Cruz Roja. (2018). *Derecho Internacional Humanitario. Respuestas a sus preguntas.* Ginebra: CICR.

- Cutrale, E. (2019). El terror yihadista. *Universitas*, (30), 88-118. Doi: https://doi.org/10.20318/universitas.2019.4837.

- D'Aspremont, J. y De Hemptinne, J. (2012). *Droit International Humanitaire*.

- Dennig, D. (2000). Cyberterrorism. En *Panel on Terrorism Committee on Armed Services U.S. House of Representatives*.

- Departamento de Defensa de los Estados Unidos. (2016). Dictionary of Military and Associated Terms. Recuperado de: https://fas.org/irp/doddir/dod/jp1_02.pdf.

- Díaz, C.M. (2006). El marco jurídico internacional de la lucha contra el terrorismo. Cuaderno de defensa 133 en Instituto Español de Estudios Estratégicos, *Lucha contra el terrorismo y Derecho Internacional*, 51-77.

- Díaz de Terán, M. (2013). *Lecciones de Teoría del Derecho*. Navarra: Universidad de Navarra.

- Diez de Velasco, M. (2001). *Instituciones de Derecho Internacional Público*. Madrid: Editorial Tecnos.

- Dobbins, J., “et al”. Cibersecurity: En: *Choices for America in a Turbulent World: Strategic Rethink, RAND Corporation*. (2015), pp. 57-88.

- ENISA. (2017). European Union Agency for Network and Information Security. Threat Landscape Report 2016. Recuperado de: https://www.enisa.europa.eu/ publications/enisa-threat-landscape-report-2016.

- Gamarra, R. (1995). *Terrorismo: tratamiento jurídico.* Lima: Instituto de Defensa Legal.

- Gasser, H. (2002). “Actos de terror, ‘terrorismo’ y Derecho Internacional Humanitario”. *Revista Internacional de la Cruz Roja*, (163).

- Gaviña, S. (25 de setiembre de 2017). «Producciones Daesh», la máquina propagandística del terror. *ABC Internacional.* Recuperado de: https://www.abc.es/internacional/abci-producciones-daesh-maquina-propagandistica-terror-201601241221_noticia.html

- Gil, R. (2012). El vacío legal del ciberespacio. *Revista de Aeronáutica y Astronáutica*, (817), 849-851.

- Gómez, A. (2012). El ciberespacio como escenario del conflicto. Identificación de las amenazas. En J.R. Casa (Ed.), *El Ciberespacio. Nuevo escenario de confrontación*, 170-203.

- Guimón, P. (2019).Trump dice que el Estado Islámico "habrá desaparecido esta noche". *El País.* Recuperado de: https://elpais.com/
- internacional/2019/03/20/estados_unidos /1553115601_727323.html.

- Gutiérrez, H. (2014). *Elementos de Derecho Internacional Humanitario*. Eudeba.

- Hoffman, B. (1999). *A mano armada. Historia del terrorismo*. Madrid: Editorial Espasa Calpe.

- Horgan, J. (2006). *Psicología del Terrorismo: cómo y por qué alguien se convierte en terrorista*. Barcelona: Gedisa.

- Ibañez, F. (2014). Los cuatro jinetes del terrorismo internacional. *Cuadernos de Pensamiento Político,* (42): pp.67-83.

- Kingsley, P. (2014). Who is behind Isis's terrifying online propaganda operation. *The Guardian.* Recuperado de: http://www.theguardian.com /world /2014 /jun/23/ who-behind-isis –propaganda-operation-iraq.

- Laqueur, W. (1987). *The Age of Terrorism.* Boston: Little Brown.

- Lawand, K. (2006). *Guia para el examen jurídico de las armas, los medios y los métodos de guerra nuevos*. Ginebra: Comité Internacional de la Cruz Roja.

- López, P. (2006). *El ciberespacio y su ordenación*. Madrid: Difusión jurídica y temas de actualidad.

- López de Turiso, J. (2012). La ciberdefensa: Un nuevo frente, una nueva necesidad ¿Qué es el ciberespacio?. *Revista de Aeronáutica y Astronáutica*, (817), 837-838.

- López-Jacoíste, E. (2018). El Estado Islámico y el Derecho Internacional Humanitario. En Gutiérrez, C. y Cervalli, M. (Dir.). *El Estado Islámico (DAESH). ¿Aprenderemos la lección?* (pp.225-299). Valencia: Tirant Humanidades.

- Lutz, B. y Lutz, J. Loc. Cit.; Torres, M. y Jordán, J. En: Jordán, J. (2013). Manual de Estudios Estratégicos y Seguridad Internacional.

- Masana, S. (2002). *El ciberterrorismo: ¿una amenaza real para la paz mundial?*(Tesis de maestría). FLACSO, Argentina.

- Olier, E. (2013). Inteligencia estratégica y seguridad económica. Cuaderno de defensa 162 en Instituto Español de Estudios Estratégicos, *La inteligencia económica en un mundo globalizado,* 9-31. Recuperado de:http://www.ieee.es/Galerias/fichero/cuadernos/CE_162_La_inteligencia_economica_en_un_mundo_globalizado.pdf.

- Organización de Naciones Unidas. (2004*). Informe del Grupo de alto nivel sobre las amenazas, los desafíos y el cambio: un mundo más seguro: la responsabilidad que compartimos (A/59/565).* Recuperado de: https://undocs.org/es/ A/59/565.

- Organización de Naciones Unidas. (2006). *Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo (A/60/825).* Recuperado de: https://undocs.org/es/A/60/825.

- Orti, J. (2012). Introducción. Monografía del CESEDEN 79 del Centro Superior de Estudios de la Defensa Nacional del Ministerio de Defensa, *Terrorismo Internacional:enfoques y percepciones,* 9-25.

- Pastor, O., Pérez, J., Arnáiz, D. y Taboso, P. (2009). Seguridad nacional y ciberdefensa. Cuadernos Cátedra ISDEFE-UPM 6. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones. Recuperado de: http://catedraisdefe.etsit.upm.es/wp content/uploads/ 2010/07/CUADERNO-N%C2%BA-6.pdf.

- Pérez, A. (2020). Ciberterrorismo, ¿una nueva amenaza?. Documento de Opinión 106/2020 en Instituto Español de Estudios Estratégicos. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/ 2020/DIEEEO106_2020AMAPER_ciberterrorismo.pdf

- Pérez, M. (2006). Terrorismo y conflictos armados. La prohibición de los actos terroristas por el Derecho Internacional Humanitario. Cuaderno de defensa 133 en Instituto Español de Estudios Estratégicos, *Lucha contra el terrorismo y Derecho Internacional*, 79-102.

- Pino, E. (2014). El Hacktivismo: entre la participación política y las tácticas de subversión digital. *Razón y palabra* (88), *26.*

- Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO*, (20), 80-93. Doi: http://dx.doi.org/ 10.17141/urvio.20.2017.2563.

- Rapoport, D. (Junio de 2004). *Las cuatro oleadas del terrorismo moderno. Conferencia llevada a cabo por la Fundación Manuel Jiménez*, Zaragoza.

- Reinares, F. (2003). *Terrorismo global*. Madrid: Taurus.

- Reguera, J. (2015). Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario. *Resi*. Recuperado de: http://www.segu ridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario#_ftn21.

- Ruiz de Azcárate, J. (2015). *Islam, terrorismo y medios de comunicación,* Madrid: Instituto Español de Estudios Estratégicos. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO092015_AmenazaCiberataques_Fco.Uruena.pdf.

- Salmón E. (2004). *Introducción al Derecho Internacional Humanitario*: Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú.

- Salmón, E. (2012). *Introducción al Derecho internacional humanitario*: Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú.

- Sánchez, F. (2019). *El Estado Islámico: ¿Un verdadero Estado? Estatalidad y responsabilidad desde el 2014 hasta la actualidad.*(Trabajo de Fin de Grado). Universidad de Sevilla: Sevilla.

- Schmid, A. (2012). The Revised Academic Consensus Definition of Terrorism. The *Perspectives on Terrorism*, *6*(2). Recuperado de:

http://www.terrorismanalysts.com/pt/index.php/pot/article/view/schmid-terrorism-definition/html.

- Schmitt, M. (2002). La guerra de la información: los ataques por vía informática y el jus in bello. *Revista Internacional de la Cruz Roja*, (846), 365 – 399.

- Subijana, I. (2008). El ciberterrorismo: Una perspectiva legal y judicial. *Eguzkilore 22*, 169-187. Recuperado de: https://addi.ehu.es/ handle/10810/24999.

- Suñe, E. (2009). Los Derechos Humanos en el Ciberespacio: La Declaración de Derechos del Ciberespacio. En ASIMELEC, *Derecho informático, electrónico y de las comunicacionesactas de la II Convención Internacional de Derecho Informático* (39-64). Madrid: ASIMELEC.

- Ticehurst, R. (1997). La cláusula de Martens y el derecho de los conflictos armados*. Revista Internacional de la Cruz Roja.* Recuperado de: https://www.icrc.org/spa/resources/documents/misc/5tdlcy.htm.

- Urueña, F. (2015). Ciberataques, la mayor amenaza actual. Documento de Opinión 09/2015 en Instituto Español de Estudios Estratégicos. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/ DIEEEO0920 15_AmenazaCiberataques_Fco.Uruena.pdf.

- Vidal, J. (2003). *La crisis del Islam: guerra santa y terrorismo.* Barcelona: Ediciones B.

- Weimann, G. (2007).Terror on the Internet: The New Arena The New Challenges. International Affairs. *Royal Institute of International Affairs*, (83), 2. pp. 386 -387.