FACULTAD DE DERECHO

LA RESPONSABILIDAD INTERNACIONAL DEL ESTADO COMO CONSECUENCIA DE LOS CIBERATAQUES UTILIZADOS COMO MÉTODO DE COMBATE A LA LUZ DEL DERECHO INTERNACIONAL HUMANITARIO

TESIS DOCTORAL

Autora: Lda. Dª Ana Pilar Velázquez Ortiz

Directora: Profª Dra. María Susana De Tomás Morales

Madrid
Abril 2017

"La novedad del hombre no reside tanto en las adquisiciones técnicas a las que se ha llegado en la actualidad, sino en la capacidad de usarlas con espíritu nuevo. En la época del robot, hay mucha más necesidad de hombres responsables".

S. Juan Pablo II.

Discurso dirigido a Oficiales y Alumnos de la Escuela de Aplicación del Ejército.

Turín, 1988

AGRADECIMIENTOS

El presente trabajo de tesis doctoral ha podido realizarse gracias al apoyo de numerosas personas con las que he podido compartir el interés por la investigación científica y, muy especialmente, por el objeto de la misma.

De entre todas ellas, es obligada la mención a mis primeros Jefes del Cuerpo Jurídico Militar, el General Auditor D. Gonzalo Zarranz Domenech y el Coronel Auditor D. Salvador Torres Ballesteros, quienes me ofrecieron la oportunidad de participar en la primera conferencia sobre aspectos legales de ciberdefensa, celebrada en el Centro de Excelencia de Ciberdefensa de Tallin y que me permitió conocer, de primera mano y en el momento incipiente, los interrogantes que comenzaba a plantear este nuevo método de combate, desde el punto de vista jurídico.

Asimismo, en el desarrollo de esta investigación ha resultado fundamental la ayuda del Asesor General del Cuerpo Jurídico Militar, el General Consejero Togado D. Juan Manuel García Labajo, quien, desde el primer momento, compartió mi entusiasmo por el presente trabajo de investigación, facilitándome la participación en las Jornadas sobre Ciberdefensa celebradas en el Centro de Estudios Superiores de la Defensa Nacional, lo que me ha permitido mantener un contacto directo con los principales investigadores en la materia. Asimismo, gracias a su interés, he tenido, a lo largo de esta labor investigadora, la oportunidad de participar en la Conferencia de la Haya celebrada con motivo de la preparación del Segundo Manual de Tallin, liderada por el Centro de Excelencia de OTAN, donde pude intercambiar ideas con el Profesor M. Schmitt, autor y editor del primer Manual de Tallin, obra de referencia en la materia.

También es de justicia agradecer a los responsables del Mando Conjunto de Ciberdefensa y, especialmente, al Teniente Coronel Gómez de Agreda, su generosidad a la hora de contar con mi participación en la presentación de los aspectos legales de la ciberdefensa, en las Jornadas que este Mando ha celebrado

a lo largo de este periodo investigador y que me ha facilitado el acceso a los especialistas en el ámbito técnico de la ciberdefensa.

Igualmente, he de agradecer encarecidamente el apoyo moral, tan necesario en el acometimiento de un trabajo de investigación como éste y que, en todo momento, he recibido de mis padres, quienes me inculcaron el amor por el esfuerzo y el afán de superación. También he de dar las gracias a mi hermana, que siempre será un referente intelectual y moral.

Y, como no, a todos mis amigos, quienes no puedan ser nombrados, como se merecerían, por ser tan numerosos –afortunadamente-, y que han vivido el proceso de elaboración de esta tesis como propio, ofreciéndome su aliento cada vez que lo he necesitado. Gracias a todos.

En último lugar y no por ello menos importante, quisiera mostrar mi más profundo y sentido agradecimiento a la Profesora Dra. Dª Susana De Tomás Morales. Si normalmente es difícil expresar el agradecimiento únicamente con palabras, en este caso, lo es aún más. Nada de lo conseguido hubiera sido posible sin su tesón, rigor académico, paciencia y largas jornadas de trabajo. A ella, solamente, se deben los aciertos que en esta investigación se hayan conseguido. Ha sido mi mentora responsable, directora entregada y amiga entrañable. Espero que el futuro nos regale muchos más años de amistad en los que me seguiré esforzando por corresponder a todo lo recibido de su parte.

LISTADO DE ACRÓNIMOS

CAQ Convención Armas Químicas.

CAB Convención Armas Biológicas.

CCDCOE Cooperative Cyber Defense Centre Of Excellence.

CDI Comisión Derecho Internacional.

CERT Computer Emergency Response Team.

CICR Comité Internacional Cruz Roja.

CIJ Corte Internacional de Justicia.

CNA Computer Network Attack.

CND Computer Network Defense.

CNE Computer network exploitation

CON Computer Network Operation.

CPM Código Penal Militar.

DIH Derecho Internacional Humanitario.

DDoS Distributed Denial of Service.

ENC Estrategia Nacional Ciberseguridad.

ESN Estrategia Seguridad Nacional.

INCIBE Instituto Nacional Ciberseguridad.

IP Internet Protocol.

LAR Lethal Autonomous Robot.

MCCD Mando Conjunto Ciberdefensa

NAT Network Address Translation.

NATO North Atlantic Treaty Organization.

OMP Operación Mantenimiento Paz.

OTAN Organización Tratado Atlántico Norte.

PA I Protocolo Adicional I.

PA II: Protocolo Adicional II.

TIC Tecnologías Información Comunicación.

TPI Tribunal Penal Internacional.

TNP Tratado No Proliferación.

TUE Tratado Unión Europea.

UE Unión Europea.

TPAY Tribunal Penal Antigua Yugoslavia.

TOR The Onion Ring.

VPN Virtual Private Network.

WANK Worms Against Nuclear Killers

ÍNDICE

INTRODUCCIÓN……...……13
1. Objetivos……...20
2. Estructura y metodología……...22

PARTE I
EL MECANISMO DE RESPONSABILIDAD
CAPÍTULO PRIMERO. EL CIBERATAQUE CONSTITUTIVO DE UN HECHO ILÍCITO INTERNACIONAL.
1. INTRODUCCIÓN……..……...……...29
2. EL CIBERATAQUE COMO HECHO ILÍCITO INTERNACIONAL. DELIMITACIÓN CONCEPTUAL DE LOS CIBERATAQUES COMO ATAQUE ARMADO……...…...……..……...35
2.1. Estudio de los ciberataques en el contexto de un conflicto armado internacional ……..……..…….....37
2.1.1. La delimitación conceptual de los ciberataques en el ámbito de la OTAN……48
2.1.2. La delimitación conceptual de los ciberataques en el ámbito de la UE…….....52
2.2. Estudio de los ciberataques en el contexto de un conflicto armado no internacional……...56
2.3. Estudio de los ciberataques en el Código Penal Militar español….....62
3. LA OBLIGACIÓN INTERNACIONAL VINCULANTE PARA EL ESTADO. DELIMITACIÓN DEL ACERVO JURÍDICO APLICABLE A LOS CIBERATAQUES…….65
3.1 El tratamiento jurídico de internet a la vista de su condición de arma de doble uso…….……..……66

4. EL HECHO ILÍCITO COMETIDO POR ACCIÓN……..…….88
5. EL HECHO ILÍCITO COMETIDO POR OMISIÓN……...……98
5.1. La conducta omisiva de un Estado puede desencadenar un ciberataque armado, frente a otro Estado……...106
*5.1.1. La aplicabilidad de la doctrina contra insurgencia a los ataques cibernéticos lanzados fuera del control del Estado…….....*107
5.1.2.- Responsabilidad por omisión de los miembros de las Fuerzas Armadas…..……..113
6. CONCLUSIONES AL CAPÍTULO PRIMERO……..121

CAPÍTULO SEGUNDO. EL CARÁCTER INTERNACIONAL DE LA OBLIGACIÓN DE DIH VIOLADA A TRAVÉS DE UN CIBERATAQUE. ORIGEN, VIGENCIA. CONTENIDO DE LA OBLIGACIÓN INTERNACIONAL.
1. INTRODUCCIÓN…….129
2. EL CARÁCTER INTERNACIONAL DE LA OBLIGACIÓN VIOLADA…….135
2.1 Delimitación de los ciberataques ilícitos a la luz del Derecho Internacional. La respuesta jurídica a distintas actividades en la red……139
2.1.1. El hacktivismo y sus posibles implicaciones en la Seguridad nacional…..……..140
2.1.2. La ciberdelincuencia...……144
2.1.3. El ciberterrorismo……...148
2.1.4.El ciberespionaje.……152
3. LAS DISTINTAS CONSECUENCIAS DE LA VIOLACIÓN DE LA OBLIGACIÓN INTERNACIONAL, EN FUNCIÓN DEL CONTEXTO EN QUE SE PRODUZCAN CIBERATAQUES……155
3.1 La ciberguerra……...…….159
3.2 Las ciberoperaciones…….167
3.3 El ciberataque como factor potenciador de un conflicto armado……..171
4. ORIGEN DE LA VIOLACIÓN……..175
5. VIGENCIA DE LA OBLIGACIÓN……182

5.1 La posibilidad de que el ciberataque se manifieste como hecho ilícito continuado……....184
5.2 El ciberataque como hecho ilícito compuesto…..……..189
6. CONTENIDO DE LA OBLIGACIÓN INTERNACIONAL INFRINGIDA….192
6.1. Los límites impuestos por el DIH a la conducción de las hostilidades, aplicables a los ciberataques……...…….194
6.1.1. La necesidad militar del ataque……..197
6.1.2. La distinción entre civiles y combatientes……...……...201
6.1.3. La proporcionalidad del ataque……..……212
6.1.4. La prohibición de la perfidia……...227
6.1.5. El respeto a la neutralidad de terceros……232
7. CONCLUSIONES AL CAPÍTULO SEGUNDO……247

CAPÍTULO TERCERO. LA ATRIBUCIÓN DEL HECHO ILÍCITO CAUSADO POR EL LANZAMIENTO DE UN CIBERATAQUE COMO MÉTODO DE COMBATE.
1. INTRODUCCIÓN……..……...261
2. LAS ESPECIALES DIFICULTADES EN LA ATRIBUCIÓN AL ESTADO DEL HECHO ILÍCITO COMETIDO VIRTUALMENTE…..…….269
3. CIBERATAQUES ORIGINADOS POR EL ESTADO……..282
3.1. Ciberataques lanzados por órganos estatales……282
3.1.1. La responsabilidad del Estado derivada de la actuación de los miembros de las Fuerzas Armadas……..……283
3.1.2. La responsabilidad del Estado como consecuencia de actos no autorizados. Los llamados actos ultra vires……...……..293
3.2. La responsabilidad en que incurre el Estado que presta ayuda o asistencia…….297
4. CIBERATAQUES GENERADOS POR AGENTES NO ESTATALES…..……..304
4.1. Atribución al Estado del hecho ilícito cometido por empresas privadas…..310
4.1.1. El papel de las empresas tecnológicas en el conflicto……..……312
4.1.2.El papel de las empresas que conforman las infraestructuras crñiticas como víctimas de un ciberataque……...…320

4.2. Los cibervoluntarios en el conflicto armado……..330
4.2.1. La atribución del hecho ilícito cometido por ciberterroristas en el conflicto armado……..…….....332
4.2.2. La atribución del hecho ilícito cometido por individuos o grupos organizados……...340
5. CONCLUSIONES AL CAPÍTULO TERCERO……..……366

PARTE II

LAS CIRCUNSTANCIAS O CAUSAS QUE EXCLUYEN LA ILICITUD DEL CIBERTAQUE UTILIZADO COMO MÉTODO DE COMBATE

CAPÍTULO CUARTO. LA NATURALEZA IMPERATIVA DE LAS NORMAS DE DIH QUE CALIFICARÍAN A UN CIBERATAQUE COMO UN MÉTODO DE COMBATE PROHIBIDO.

1.INTRODUCCIÓN……..……377
2. CARACTERES DEL *IUS COGENS* Y SU CONSTATACIÓN EN LAS NORMAS PROHIBITIVAS DE DIH RELATIVAS A LOS MÉTODOS DE COMBATE……..……381
2. 1. La universalidad de las normas de *ius cogens*……..….381
2.1.1. El consenso generalizado en su proceso de formación……..381
2.1.2. La aplicación universal de las normas imperativas……...385
2.2. La imperatividad de las normas de *ius cogens*……...386
2.3. La superioridad de las normas de *ius cogens*……..388
3. CRITERIOS DE IDENTIFICACIÓN DE LAS NORMAS DE IUS COGENS…397
3.1. La necesidad militar…….....403
3.2. La obligación de distinguir entre civiles y combatientes…….406
3.3. La obligación de observar la proporcionalidad en el ataque……..407
3.4. La prohibición de la perfidia……409
3.5. La obligación de respetar la neutralidad de terceros Estados……410

3.6. Otras violaciones graves…….412
4.CONSECUENCIAS DE LA VIOLACIÓN DE UNA NORMA IMPERATIVA……..413
5. CONCLUSIONES AL CAPÍTULO CUARTO…….417

CAPÍTULO QUINTO: OTRAS CAUSAS QUE EXCLUYEN LA ILICITUD DE LAS CIBERATAQUES QUE CONTRAVENGAN EL DIH.
1. INTRODUCCIÓN……421
2. ESPECIAL CONSIDERACIÓN A LA LEGÍTIMA DEFENSA COMO POSIBLE CAUSA JUSTIFICATIVA DEL HECHO ILÍCITO INTERNACIONAL……...425
2.1. La necesidad de la defensa y el momento de ejercerla…….427
2.2. La proporcionalidad en la respuesta por medios cibernéticos y convencionales……..442
3. OTRAS CAUSAS QUE EXCLUYEN LA ILICITUD……451
3.1. El consentimiento prestado por el Estado durante el conflicto armado…..451
3.2. Las contramedidas y su relación con las represalias bélicas……...455
3.3. La fuerza mayor……..463
3.4. El peligro extremo……...468
3.5. El estado de necesidad.……...471
4. CONCLUSIONES AL CAPÍTULO QUINTO……474

CONCLUSIONES FINALES……..…….477

BIBLIOGRAFÍA BÁSICA CONSULTADA….....493

JURISPRUDENCIA……..508

DOCUMENTACIÓN……...510

INTRODUCCIÓN

La irrupción de internet en el siglo pasado y su rápida extensión en escasas décadas ha supuesto una revolución en determinados sectores de nuestra vida cotidiana cuyos beneficios no resulta difícil identificar. La inmediatez que permite este medio en la gestión de las comunicaciones personales y en las transacciones comerciales es evidente. Sin perjuicio de que todavía no podemos conocer cuáles serán las consecuencias físicas e intelectuales que, individualmente, vayamos a soportar a largo plazo, como resultado de su uso y que aún están siendo objeto de estudio por la ciencia[1], lo cierto es que se trata de un medio de comunicación, cuyas posibilidades de utilización parecen tan ventajosas como ilimitadas.

Sin embargo, como cualquier innovación puesta en manos del hombre, su uso en perjuicio de determinados intereses, también humanos, se ha visto pronto y de forma clara. La comisión cibernética de algunos delitos junto con la aparición de nuevas formas delictivas, como el cibersecuestro[2] o la difusión de propaganda terrorista, a través de determinados canales de internet y de las redes sociales, son sólo algunas de sus manifestaciones. Y, como tradicionalmente ha ocurrido, las novedades tecnológicas suscitan un debate en torno a su regulación y a las consecuencias que pudiera generar el uso de las mismas[3] del que internet no ha sido ajeno.

---

[1] Al respecto, resultan particularmente interesantes las conclusiones alcanzadas en el estudio, CARR, N., The shallows. What the internet is doing to our brains. Norton and Company Inc. New York, 2010.

[2] Este es el llamado cibersecuestro por el que se pide un rescate económico, al objeto de que el legítimo usuario del sistema pueda volver a utilizarlo. Al respecto, puede consultarse el Boletín Informativo núm. 21 de 2016, del Mando Conjunto de Ciberdefensa, que define el cibersecuestro en los siguientes términos: "*Ransomware es un término proveniente del inglés para indicar un tipo de software malicioso que bloquea el acceso a los datos almacenados en su computadora. De esta forma el atacante exige una recompensa para recuperar su información. La forma en que el ransomware trabaja es cifrando la información con una llave que únicamente el atacante conoce. Sus datos siguen en el equipo, solamente que ya no los puede leer*". Definición recogida en el Boletín de Información del Mando Conjunto de Ciberdefensa núm.21 de 2016, del sitio web: http://www.skalant.com/es/redes/23-ransomware-cuidado-con-el-secuestro-de-informacion. Fecha de consulta, enero de 2017.

[3] Como afirma MARÍN LÓPEZ, "*El progreso ha cambiado, así, completamente la relación del hombre con su medio; las nuevas actividades son ya origen de un riesgo aceptado por todos y recogido en acuerdos internacionales, aunque la naturaleza exacta y la extensión de la responsabilidad están sujetas a discusión*",

La popularización del uso de internet, además, ha supuesto que, a los dominios, hasta ahora conocidos, en los que los individuos y los Estados desarrollaban sus relaciones se añadiera uno nuevo, el virtual[4]. La peculiaridad que el mismo presentaba se manifiestaba principalmente en que se trata de un espacio sin fronteras ni delimitación física que, además, ofrecía la posibilidad añadida del anonimato. Cuando en la primavera del año 2007, Estonia quedó seriamente afectada, como consecuencia de los ciberataques recibidos, se puso de manifiesto que internet planteaba una serie de retos, más allá de los meramente técnicos. Con posterioridad a aquel suceso, el fenómeno de los ciberataques no ha visto disminuida su protagonismo. Antes al contrario, éste se vió aumentado cuando el lanzamiento de los mismos comenzó a realizarse en distintos contextos bélicos, abriendo así una puerta, a la llamada "ciberguerra". La constatación de alteraciones en los sistemas informáticos de los ejércitos en combate, durante los conflictos de Georgia y Ucrania, reveló cómo las nuevas capacidades militares exigían que el Derecho Internacional ofreciera una respuesta innovadora, con tanta rapidez como eficacia.

Con anterioridad a estos concretos incidentes, los Estados ya habían tenido en cuenta la posibilidad de que el ciberespacio constituyera una nueva amenaza y que las amenazas a la Seguridad y a la Defensa Nacional podían proceder del mundo virtual[5], de forma que era necesario afrontarlas desde un punto de vista

---

MARIN LÓPEZ, A. *Aspectos actuales de la responsabilidad internacional*. Estudios de Derecho Internacional en Homenaje al profesor Miaja de la Muela, vol. II. Tecnos. Madrid, 1979; pp. 815-836, en particular, p. 816.

[4] El ciberespacio ha sido definido por OTTIS y LORENTS, como "*a time dependent set of interconnected information systems and the human users that interact with these systems*". OTTIS, R., LORENTS, P., *Cyberspace: Definition and Implications*. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2010. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited; pp. 267-270, en particular, p. 269.

[5] Así puede comprobarse tanto en la Estrategia Española de Seguridad de 2011, como en la Estrategia de Seguridad Nacional de 2013. En ambos documentos aparecen expresamente recogidas las ciberamenazas. GOBIERNO DE ESPAÑA. Estrategia Española de Seguridad. Una responsabilidad de todos. Gobierno de España. 2011; pp. 65-70 y, GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional. Un Proyecto Compartido, Presidencia del Gobierno, 2013. Documento publicado por el Gobierno de España; p.26.

integral y, en esa tarea, la llamada ciberdefensa, comenzó a tener un papel fundamental[6].

En un principio, el nuevo concepto de ciberdefensa podría parecer poco concreto, pues las capacidades militares que el mismo engloba son muy diversas. La posibilidad de afrontar un conflicto bélico a través de métodos exclusivamente cibernéticos es una de ellas y, de esta forma podría librarse, en un futuro, una ciberguerra. Pero, además, esas capacidades de ciberdefensa permiten una combinación con los métodos de combate convencionales, de tal manera que, en un conflicto armado, estos últimos sean utilizados junto con el desarrollo de ciberoperaciones. Es decir, operaciones cibernéticas que puedan influir, directamente, en las capacidades militares del adversario, sean éstas virtuales o no. Tal como ocurrió en los conflictos que han sido citados, las Fuerzas Armadas podrán valerse de sus métodos cibernéticos para lograr una ventaja militar que, a través de métodos de combate convencionales, supondría una mayor dificultad. En este sentido, parece evidente que el lanzamiento de un ciberataque, *a priori*, ofrece la posibilidad de combatir asumiendo un menor riesgo de bajas humanas e incluso un menor coste económico. Pues bien, en el desarrollo de estas ciberoperaciones, será donde el lanzamiento de ciberataques se dará con mayor frecuencia.

Sin embargo, la constatación de ciberataques no se da exclusivamente en situaciones de beligerancia. Por el contrario, los ataques informáticos que a diario se producen se manifiestan con mayor frecuencia en situaciones que no corresponden a ningún conflicto. Por este motivo resulta especialmente interesante plantarse hasta qué punto un ciberataque que sea lanzado sin que previamente exista un conflicto bélico, puede llegar a desencadenarlo.

Ya, con anterioridad a que se produjeran los ataques informáticos, el auge de nuevos métodos de combate había supuesto una distorsión en el desarrollo de

[6] Un ejemplo de ello lo constituyen las distintas Estrategias de Ciberseguridad publicadas por los Estados, que pueden consultarse en la página web del Centro de Excelencia de Ciberdefensa de OTAN, en lo que a sus Estados miembros se refiere. *Cyber Security Strategy Documents*, disponible en el sitio web: https://ccdcoe.org/strategies-policies.html. Fecha de consulta, enero de 2106.

los conflictos armados, dando lugar a los denominados conflictos asimétricos[7] y conflictos híbridos[8]. Los conflictos asimétricos se habían puesto de manifiesto como consecuencia del desequilibrio entre las partes combatientes, más allá de la lógica disparidad de capacidades militares que puede darse en cualquier contienda[9]. Desde el punto de vista militar, el conflicto asimétrico fue estudiado y afrontado, a través de la aplicación de la doctrina militar, relativa a la contrainsurgencia[10].

El conflicto híbrido, por su parte, se define entre otras notas, por la intervención de agentes no estatales. Esta participación supone la introducción de un factor adicional, de entre los muy diversos que, de forma coordinada, participan en el conflicto, sin utilizar métodos de combate convencionales[11].

Por otra parte, si hasta ahora la separación entre las materias propias de la Seguridad Nacional y de la Defensa Nacional parecía clara, en este momento esa

---

[7] En relación a los conflictos asimétricos, puede consultarse GEISS, R. *Las estructuras de los conflictos asimétricos*. Revista Internacional de la Cruz Roja, núm. 864. Diciembre de 2006; pp. 1-23.

[8] Un ejemplo de estos conflictos híbridos, lo constituye el librado entre Rusia y Ucrania, en el que se manifiestan diversos factores: "*Rusia, aparentemente, ha empleado, para alcanzar sus objetivos políticos, una mezcla de operaciones especiales, presión económica, agentes de inteligencia, instrumentalización del flujo de gas natural, ciberataques, guerra de información y empleo de fuerza militar convencional como medida de presión/disuasión. Todo ello, perfectamente sincronizado formando parte de un plan de operaciones… lo cual se puede enmarcar totalmente dentro del concepto que se ha dado en llamar "guerra híbrida*". SÁNCHEZ HERRÁEZ, P. La nueva guerra híbrida: un somero análisis estratégico. Documento de Análisis 54/2014. 29 de octubre de 2014. Instituto Español de Estudios Estratégicos. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEEA54-2014_NuevaGuerraHibrida_PSH.pdf Fecha de consulta, mayo de 2015.

[9] Como afirma PELLICER BALSALOBRE, "*La verdadera asimetría no solo reside en las diferencias de poderío y organización militar de las fuerzas beligerantes, también en las tácticas, en los valores y en los objetivos. En la guerra asimétrica no prima el exterminio del enemigo, basta con el condicionamiento de su comportamiento político mediante el miedo y la intimidación*". PELLICER BALSALOBRE, J.M, El recurso humano en la doctrina para los escenarios de guerra asimétrica. Documento Marco 6/2017, 3 de abril de 2017. Instituto Español de Estudios Estratégicos; p.6. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_marco/2017/DIEEEM06-2017_Guerra_Asimetrica_JoaquinPellicer.pdf. Fecha de consulta, abril de 2017.

[10] SÁNCHEZ GARCÍA, F., *El empleo de la fuerza en el conflicto asimétrico*. Revista Ejército, núm. 836. Diciembre 2010; pp. 22-30.

[11] El conflicto híbrido fue "*Definido originalmente en el año 2002 para advertir de las tácticas empleadas por la insurgencia chechena contra el ejército ruso durante la Primera Guerra de Chechenia (1994-96)*" y "*el término guerra híbrida fue empleado por primera vez de manera oficial en la Estrategia Nacional de Defensa estadounidense de 2005 para explicar la combinación de dos o más amenazas de tipo tradicional, irregular, catastrófico o disruptivo*". COLOM PIELLA, G. *¿El auge de los conflictos híbridos?* Documento de Opinión 120/2014. 24 de octubre de 2014. Instituto Español de Estudios Estratégicos; p.2. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO120-2014_GuerrasHibridas_Guillem_Colom.pdf. Fecha de consulta, enero de 2015.

separación conceptual de los dos ámbitos es difusa, como consecuencia de diversos factores. Los supuestos de terrorismo internacional son, quizás, el caso más evidente. La conceptuación de algunos atentados terroristas como ataques armados, en el sentido mantenido tradicionalmente por las Naciones Unidas, ha abierto una brecha en la seguridad jurídica internacional, al introducir no pocas incógnitas, en la calificación jurídica de estos hechos[12].

Desde el punto de vista militar, por lo tanto, el ciberespacio se muestra como un dominio más en el que ejercer las capacidades de las Fuerzas Armadas. Una vez asumida la posibilidad de que se llegue a librar un combate virtual, obliga a plantearse, en definitiva, qué ha de entenderse, por ciberataque y cuáles han de ser los límites jurídicos, que las Fuerzas Armadas tendrán que respetar cuando decidan utilizar los ciberataques, como método de combate, durante un conflicto armado.

En esta labor, uno de los principales retos a los que hay que hacer frente es, por lo tanto, delimitar en qué supuestos las incidencias informáticas a las que, coloquialmente, se denominan ciberataques, también lo son desde un punto de vista jurídico. El concepto de ataque armado sigue siendo una cuestión merecedora de estudio y, todavía más, cuando nos encontramos ante la posibilidad de que el ataque sea perpetrado por medio de un método de combate novedoso. Por otra parte, no puede olvidarse que se trata de un método de combate que se halla al alcance de una gran pare de la población, al menos en los Estados más desarrollados.

En consecuencia, resulta clave atender, en primera instancia, al concepto de ataque armado y delimitar si, en el mismo, puede ser incluido el que se realice a través de internet. El principal obstáculo que aquí se presenta lo constituye la gran cantidad de manifestaciones que se dan diariamente través de la red, con un fin ilícito. La utilización de internet con fines bélicos es la más grave de esas manifestaciones, pero no puede obviarse el aumento de la ciberdelincuencia o el uso de internet con fines terroristas, entre otros. Por ese motivo, la distinción

[12] EYMAR ALONSO, C. *Estados Unidos y la cuestión de la legítima defensa preventiva*. Grupo de Estudios Estratégicos. Disponible en el sitio web:http://www.gees.org/articulos/estados-unidos-y-la-cuestion-de-la-legitima-defensa-preventiva. Fecha de consulta, enero de 2014.

entre los ataques cibernéticos que pueden ser calificados jurídicamente como ataques armados y otros, a los que se tendrá que dar respuesta por el Derecho Internacional general o por las normas penales de cada Estado, es la principal tarea en esta parte del proceso. De otro modo podría ocurrir que se calificara jurídicamente como ataques armados a actividades que no lo son. En este sentido, si algo ha puesto de manifiesto el uso malicioso de internet es su capacidad de influir en la opinión pública, de forma que no se puede desdeñar la posibilidad de que, a través de la red, puedan provocarse estados de opinión y reacciones populares que afecten a la seguridad interna de un Estado. La posibilidad de que estas actividades sean calificadas jurídicamente de forma errónea es tan evidente como arriesgada y obliga a proponer unos criterios delimitadores que aclaren esta cuestión.

Por otra parte, parece evidente que un uso ilícito de este método de combate, por parte del Estado, podría originar su responsabilidad internacional. Así pues, resulta obligado, en este estudio, atender a la obligación internacional, cuya violación origina la responsabilidad internacional del Estado. Surge aquí el segundo de los retos, pues la posibilidad real de que internet sea utilizado como método de combate no ha ido seguida de su correspondiente regulación por parte del Derecho Internacional. La ausencia de una normativa expresa internacional, evidencia otro factor de inseguridad jurídica que se tendrá que subsanar en un futuro. Mientras el mismo persista, es necesario que los Estados que entren en combate utilizando armas cibernéticas, se sometan a la legalidad internacional, aplicable a los conflictos. De lo contrario, podría entenderse que el uso de las ciberarmas constituye una ventaja adicional, desde el punto de vista jurídico, al entender que la ausencia de legalidad internacional permite un uso ilimitado. Por este motivo parece necesario cuestionarse si, al igual que ha ocurrido tradicionalmente con otras armas novedosas, internet puede ser objeto de aplicación de las normas relativas al combate de Derecho Internacional Humanitario (en adelante, DIH) en tanto no se produzca una regulación expresa de su uso en este ámbito.

En consecuencia, es especialmente relevante partir de un concepto preciso de ciberataque armado pues, al delimitar la regulación jurídica que sea aplicada a los mismos, nuevamente, hay que dejar de lado la que rige en el caso de todos aquéllos ataques cibernéticos que no son ataque armado y a los que el ordenamiento jurídico ya ha dado respuesta. Esta distinción, ya se apuntaba complicada por la citada relación entre las cuestiones de seguridad interna y los factores de riesgo, que amenazan a la Defensa de un Estado. En este aspecto, es evidente que determinados usos ilícitos de internet ya han sido encuadrados en el ámbito penal. Es decir, por muy violenta que, desde el punto de vista social, resulte una protesta que se realice por internet y, aun cuando se tengan indicios de que otro Estado podría estar apoyándola, no siempre se darán las circunstancias que permitan calificar dicha situación como ciberataque armado. De hecho, en los ataques informáticos que han tenido más repercusión mediática en el ámbito internacional podría parecer, a primera vista, que estas condiciones estaban presentes. Sin embargo, en ellos se puso de manifiesto la tercera de las dificultades con las que la Comunidad Internacional va a enfrentarse en esta tarea: la atribución del hecho ilícito.

La utilización de un método de combate tan singular como internet supone una dificultad añadida en la siempre difícil tarea de atribuir el hecho ilícito. Por esta razón, el estudio de las cuestiones relativas a la atribución del hecho ilícito requiere contemplar la situación desde una perspectiva nueva por varios motivos. En primer lugar, porque si consideramos que internet puede ser utilizado como un método de combate, es evidente que se trata de un arma al alcance de millones de personas. En segundo lugar y, como consecuencia de lo anterior, nos encontraremos ante una situación en la que la participación de personal civil resultará más sencilla y frecuente que con otro método de combate. De forma evidente, la unión de ambos factores supondrá un aumento en la incertidumbre, en relación a la atribución del hecho ilícito.

Por último, la aplicación a los ciberataques, de las normas relativas a los conflictos armados impone el estudio de esta materia, analizando su posible naturaleza imperativa. Las causas de exención de la ilicitud del hecho han de ser

examinadas a la luz de esta cuestión, en tanto que las mismas carecerán de toda efectividad frente a la violación de una norma de *ius cogens*.

1. Objetivos.

El objetivo principal que se aborda por medio de este estudio supone la aportación de un análisis a las cuestiones clásicas, relativas a la responsabilidad internacional del Estado, ofrecido desde la perspectiva que este nuevo método de combate suscita. Se trata de delimitar, por lo tanto, la incidencia que puede tener el uso de los ciberataques como método de combate, en la responsabilidad internacional del Estado que haga uso de los mismos contraviniendo la legalidad internacional. Para ello, es necesario abordar una nueva interpretación de las materias tradicionales relativas al concepto de ataque armado, la licitud de los métodos de combate, la aplicación del DIH, las cuestiones relativas a la comisión del hecho ilícito y su atribución, así como la reparación del daño ocasionado por el hecho ilícito y las causas de exclusión de ilicitud para determinar, en definitiva, en qué supuestos es exigible la responsabilidad internacional del Estado, cuando internet se utilice como un método de combate.

Para la consecución de este objetivo principal de la presente investigación, debemos atender a la consecución de dos grandes objetivos específicos. El primero de ellos será atender a las cuestiones relativas al mecanismo de responsabilidad internacional del Estado, como consecuencia del lanzamiento de ciberataques prohibidos por el DIH y el segundo de ellos, el examen de las circunstancias o causas que excluyen la ilicitud del ciberataque utilizado como método de combate.

El primer objetivo específico planteado, impone realizar un análisis del concepto de ataque armado, desde una nueva perspectiva que permita valorar si los ataques cibernéticos pueden ser incluidos en dicho concepto. En consecuencia, procederá examinar, posteriormente, los elementos constitutivos del hecho ilícito internacional, por violación del Derecho Internacional general y, con carácter especial, del conjunto normativo del DIH. Se trata así de determinar

si el hecho ilícito, por acción y por omisión, puede cometerse cuando se lance un ciberataque como método de combate.

Una vez determinada la naturaleza jurídica de los ataques cibernéticos, se abordará el examinen de la aplicabilidad a los mismos del Derecho Internacional general y del DIH, para determinar en qué supuestos los ciberataques constituyen un método de combate prohibido por el DIH. Asimismo, se atenderán los mecanismos de reparación pertinentes a cada una de las violaciones de DIH, cuando éstas se produzcan como consecuencia del uso de un ciberataque como método de combate. La aplicación del DIH a los conflictos cibernéticos, así como a las operaciones cibernéticas desarrolladas en el transcurso de conflictos tradicionales, ha sido objeto de debate por parte de la doctrina internacionalista. Sin embargo, las condiciones que algunos autores entienden que han de darse en un conflicto armado para que la aplicación del DIH resulte incontrovertida, han originado una dialéctica en la doctrina internacionalista que resulta preciso esclarecer.

Además, este primer objetivo específico implicará el estudio de la atribución de responsabilidad del Estado, a la luz de las normas de Derecho Internacional pertinentes, tanto en los supuestos en que el ciberataque como método de combate prohibido haya sido cometido por agentes estatales y no estatales. Uno de los principales problemas que plantea el uso de Internet está constituido por la indagación de la autoría del ataque informático, habida cuenta la facilidad con que puede preservarse el anonimato en la red. Desde el punto de vista jurídico, esta dificultad, constituye un reto a la hora de determinar la responsabilidad por la comisión de dicho ataque. El estudio de la responsabilidad internacional del Estado, por la comisión de un hecho ilícito pasará, inevitablemente, por el estudio de los elementos de dicho mecanismo. Además, la comisión de ciberataques ilícitos en el desarrollo de la ciberguerra o de un conflicto armado convencional, podrá producirse tanto de forma deliberada como imprudente. Se atenderá, pues, a la atribución de responsabilidad al Estado, cuando el mismo, a través de sus Fuerzas Armadas cometa un hecho ilícito, por contravenir las normas de DIH aplicables a los

métodos de combate. Sin embargo, aun de forma tangencial, deberá hacerse referencia a la comisión del ilícito por particulares y su posible atribución al Estado, habida cuenta las situaciones antes mencionadas que pudieran producirse como consecuencia de la participación de civiles en el conflicto.

Para la consecución del segundo objetivo específico, se deberá atender, con carácter especial, la posible naturaleza imperativa de las normas de DIH, de la prohibición de ciberataques que no cumplan con las limitaciones establecidas por el DIH, lo que no impide que se aborden las otras causas que puedan excluir la ilicitud, entre las que adquirirá un protagonismo especial, la legítima defensa.

2. Estructura y metodología.

La consecución del objetivo principal de la investigación obliga a diferenciar en dos grandes partes diferenciadas el presente trabajo de Tesis Doctoral, a través de las cuales, podrán darse respuesta a los dos objetivos específicos, antes expuestos.

A la hora de abordar el primer objetivo específico nos encontramos no solo con la novedad del método de combate y la ausencia de normativa específica aplicable al mismo, sino al mismo tiempo, con escasas referencias doctrinales y jurisprudenciales en la materia. Por otra parte, el tema seleccionado como objeto de la presente investigación ha sido tratado, principalmente, por Organizaciones y Organismos Internacionales. En la doctrina española, son pocos los autores que hayan dedicado su estudio a este novedoso ámbito. La mayor parte de la doctrina española que, hasta la fecha ha tratado el presente tema, se ha ceñido a los aspectos técnicos de la ciberdefensa y no al tratamiento legal de la misma, cuyo estudio se ha circunscrito, principalmente, al empleo de Internet para la comisión de ilícitos penales o ciberdelitos o como medio de difusión de actividades terroristas. Las escasas referencias bibliográficas encontradas se centran, monográficamente, en aspectos concretos de la ciberdefensa, sin que se haya ofrecido un análisis integral de los aspectos técnicos y legales ni tampoco de las lecciones identificadas en la solución de controversias hasta ahora

producidas. Por ello, las fuentes doctrinales consultadas emanan, básicamente, de la OTAN.

Esta Organización cuenta con varias publicaciones en la materia, difundidas a través del Centro de Excelencia en Ciberdefensa de Tallin, Estonia. Han sido varios los estudios que dicha Organización ha patrocinado, poniendo en común el trabajo de distintos autores, mayoritariamente de origen anglosajón, que han intentado aportar una respuesta unívoca, desde el punto de vista del Derecho Internacional, a la comisión de los ciberataques. Sin embargo, la diversidad de criterios hasta ahora aportados, ha impedido que dicha Organización haya aprobado una doctrina común, aplicable por todos sus Estados miembros.

Por último, tampoco puede olvidarse la aportación doctrinal que ofrece el Comité Internacional de la Cruz Roja, en el estudio del DIH. La difusión de esta materia y la preocupación del citado Organismo por el cumplimiento del Derecho de los conflictos armados, en toda circunstancia, impone el estudio de sus documentos con carácter preeminente. A través de dicha documentación podrán abordarse las cuestiones relativas a las normas de DIH aplicables a este nuevo método de combate, así como las consecuencias de su incumplimiento.

En la tarea interpretativa analógica que se debe realizar, se tendrán presentes las grandes aportaciones de la Comisión de Derecho Internacional en relación a la responsabilidad internacional, en particular, el Proyecto de artículos sobre responsabilidad internacional del Estado y los Comentarios al mismo.

En el análisis de las distintas cuestiones que se abordan, se hará referencia a la materialización de los ataques cibernéticos, en sus distintas manifestaciones y, por lo tanto, en los supuestos en que éstos se produzcan aisladamente y también en aquéllos que se desenvuelvan dentro de un conflicto armado, sea éste de carácter internacional o no. A través de dicho examen se concluirá cuál ha de ser la norma de Derecho Internacional, aplicable al caso, atendiendo para ello al Derecho Internacional general, así como al régimen especial constituido por las normas de DIH y en qué medida resulta exigible la responsabilidad del Estado transgresor.

Para ello se partirá del análisis de situaciones que, hasta el momento, han sido constatadas y en las que, de forma evidente o indiciaria, se ha manifestado la acción de un Estado. Dicho análisis se realizará a partir del estudio normativo, doctrinal y jurisprudencial. Este acervo será sometido a una interpretación analógica para atender al contexto de los ataques cibernéticos, de forma que permita determinar la responsabilidad internacional del Estado, al ser de aplicación los elementos constitutivos del mecanismo de responsabilidad.

A la luz de los más recientes casos de los que se tiene noticia, se examinará si un ciberataque reúne las mismas características que un ataque convencional para ser conceptualizado como tal.

El capítulo primero responde, con carácter general, a la metodología expresada. El punto de partida conceptual resulta insoslayable y ha de realizarse con carácter previo a abordar la responsabilidad internacional en que pueda incurrir el Estado como consecuencia del lanzamiento de un ataque armado cibernético. Aun teniendo en cuenta que la escasa doctrina que ha abordado esta materia no resulta pacífica, en ningún caso puede aceptarse que la ausencia de previsión de un método de combate dentro de las prohibiciones del DIH, implique la posibilidad de su libre utilización, sin restricciones, por parte de los Estados.

Además, es necesario que, tal y como ya ocurrió con el uso de las armas convencionales, en primer lugar, y con las nucleares, más recientemente, el concepto de método de combate resulte incontrovertido. Por este motivo se analizará dicho concepto desde una perspectiva teórico-práctica, por cuanto no puede obviarse que ha sido un método ya utilizado en determinados conflictos a los que, inevitablemente, habrá que hacer referencia. El estudio requiere un análisis del DIH, de las aportaciones de la doctrina internacionalista y de las decisiones jurisprudenciales que, en aplicación de la analogía, han entendido que determinados métodos para hacer la guerra, que no estaban contemplados inicialmente por los Estados, habían de ser incluidos en tal categoría y a los que, por tanto, son de aplicación las pertinentes restricciones.

En el capítulo segundo, el análisis de la aplicabilidad del DIH al fenómeno de los ciberataques, partirá de las conclusiones que, de forma provisional, se hayan alcanzado en el capítulo previo. Así, una vez calificado jurídicamente el hecho ilícito - en el presente caso, el ciberataque- corresponderá determinar qué norma resulta aplicable. Únicamente de esta forma podrá seguirse un *iter* lógico que determine la posibilidad de exigir dicha responsabilidad internacional a un Estado.

Con este método se persigue esclarecer las consecuencias que tendría tanto la aplicación del DIH como la inaplicación del mismo, así como determinar si un ataque cibernético, que sea considerado un método de combate y, por lo tanto, sea objeto de aplicación del DIH, reúne o no los requisitos exigidos para ser considerado un hecho ilícito, de conformidad con el Derecho Internacional. Ello exigirá, consecuentemente, la interpretación analógica de los criterios de aplicabilidad del DIH, en relación a los métodos de combate tradicionales. La aplicación del DIH se advierte como una cuestión de mínimos, en tanto la normativa en la materia no resulte oportunamente actualizada. Por otra parte, una vez se analicen las premisas necesarias para la aplicación del DIH, podrá comprobarse que, si bien su adecuación a los ciberataques exige una labor interpretativa, ello no supone un óbice insalvable para su aplicación. El examen del Derecho Internacional general, por su parte, permitirá establecer los mecanismos de reparación que han de aplicarse cuando el hecho ilícito se cometa a través de un ciberataque utilizado como método de combate.

El capítulo tercero comparte una misma metodología. También aquí, las fuentes del Derecho utilizadas serán el Derecho Internacional general y el régimen especial de DIH. Será, asimismo, imprescindible el recurso a la jurisprudencia, a través de un enfoque que permita identificar la normativa internacional, existente en el momento de surgir los nuevos conflictos que este método de combate origina, a través de la aplicación de los criterios consolidados en decisiones jurisprudenciales. De este modo será posible atender a todas las cuestiones que se abordan en el capítulo destinado a las cuestiones de atribución del hecho ilícito.

En relación con la consecución del segundo objetivo específico antes mencionado, ha resultado necesario estructurar la segunda parte del presente trabajo de Tesis Doctoral, en dos capítulos diferenciados debido a las dificultades añadidas que presenta la atención del concepto de *ius cogens* internacional. De esta forma, en el capítulo cuarto se atenderá la naturaleza imperativa de las normas de DIH aplicables al combate, para poder determinar la exclusión de la ilicitud de un ciberataque utilizado como método de combate. Si hasta ahora ha sido necesario acudir a la interpretación analógica de la doctrina, normativa y jurisprudencia, aún se hace más necesario al abordar las normas de *ius cogens* en relación con las causas de exclusión de la ilicitud de responsabilidad internacional.

Por último, en el capítulo quinto, esta misma metodología se hace imprescindible atender, con carácter especial a la legítima defensa, como causa de exclusión de la ilicitud, por cuanto la práctica de los Estados parece querer justificar una flexibilización en torno a los requisitos exigidos por el Derecho Internacional.

Para abordar este segundo objetivo específico, además de atender a la doctrina internacionalista el Derecho Internacional general y las normas de DIH y a la jurisprudencia internacional, resultan de especial atención las aportaciones de la Comisión de Derecho Internacional, no solo en materia de responsabilidad internacional sino también, con carácter especial, los trabajos realizados en torno al *ius cogens* internacional. Por último, resulta especialmente relevante en relación al estudio de la legítima defensa, la normativa de la Unión Europea y de la OTAN.

PARTE I

EL MECANISMO DE RESPONSABILIDAD

CAPÍTULO PRIMERO. EL CIBERATAQUE CONSTITUTIVO DE UN HECHO ILÍCITO INTERNACIONAL.

1. INTRODUCCIÓN.

El planteamiento del ciberataque como hecho ilícito internacional conlleva, indefectiblemente, la atención de distintas cuestiones que, a lo largo del presente Capítulo se irán examinando, al objeto de determinar en qué supuestos un ataque informático incurre en la definición que ofrece el artículo 2 del Proyecto de artículos de responsabilidad internacional del Estado (en adelante, el Proyecto)[13]. De conformidad con el mismo, hay hecho ilícito internacional del Estado cuando una acción u omisión es atribuible al Estado y, además, constituye una obligación internacional del Estado. De este modo, resulta imprescindible comenzar el análisis de la presente cuestión examinando si es posible, infringir una obligación internacional, a través de un ataque cibernético, en el transcurso de un conflicto armado, sea éste internacional o no internacional. Para ello, asimismo, resultará determinante señalar cuál sea la obligación internacional infringida o, lo que es lo mismo, determinar el régimen jurídico aplicable a los ciberataques que se empleen en el contexto bélico.

La responsabilidad internacional del Estado por la comisión de hechos ilícitos, obviamente, no constituye una materia nueva en Derecho Internacional. Sin embargo, la aparición de nuevas armas de las que pueden valerse los Estados, a la hora de librar los conflictos en que se hallen inmersos, plantea una serie de cuestiones que sí son novedosas. Son variadas las armas que, en virtud de la tecnología más desarrollada, han ido implantándose en la escena internacional y, de entre todas estas innovaciones tecnológicas, los ciberataques, por su naturaleza y efectos, merecen una especial atención.

13Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos. Documento A/56/10. Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53º período de sesiones (23 de abril a 1º de junio y 2 de julio a 10 de agosto de 2001). Distribuido inicialmente como Documentos Oficiales de la Asamblea General, quincuagésimo sexto período de sesiones, Suplemento n.° 10.

El estudio de la responsabilidad en que pueda incurrir el Estado por la comisión de hechos ilícitos, en el uso de los ciberataques como método de combate, exige el análisis de cada uno de los elementos que conforman dicha relación jurídica de responsabilidad. Por ello, se hace necesario abordar, como cuestión previa, si los ciberataques pueden ser incluidos entre los métodos de combate de los que dispone un Estado para la salvaguarda de su Defensa Nacional.

La gran cantidad y diversidad de ataques informáticos, de los que a diario se tiene constancia, ha hecho necesario que a los mismos se dé una respuesta técnica que impida o minimice los efectos que de ellos se derivan. A esa solución, meramente material, tendrá que acompañarse la correspondiente respuesta jurídica, pues ninguna sociedad puede permitir que su ordenamiento jurídico quede ajeno a la producción de la lesión de bienes jurídicos, con independencia de que esta lesión se realice a través de nuevos métodos. Por otra parte, tampoco a la Comunidad Internacional le resulta indiferente la amenaza que para la paz y seguridad mundiales comportan determinadas actividades en la red. No obstante, es evidente que ni toda actividad cibernética resulta contraria a Derecho, ni toda actividad cibernética ilícita, puede recibir idéntica respuesta jurídica.

Con carácter previo, pues, a determinar cuáles son los hechos ilícitos que pueden conllevar la responsabilidad internacional del Estado, habrá que perfilar cuáles son las obligaciones jurídicas que los Estados han de cumplir para no incurrir en ilicitud; cuestión ésta que requiere el previo examen de la normativa a la que ha de atenerse el empleo de los ataques informáticos, cuando éstos constituyen un ataque armado.

Sin embargo, este análisis se enfrentará a la ausencia de previsión explícita de este específico método de combate. Ni el Derecho Internacional Convencional ni el Consuetudinario prevén expresamente la posibilidad de que se lleve a cabo una ciberguerra o una ciberoperación, de la misma manera que el lanzamiento de un ciberataque deberá ser examinado a la luz de los criterios que han quedado vistos antes de calificarlos jurídicamente como ataques armados. Así pues, tanto la ausencia de prohibición del uso de internet en el desarrollo de un conflicto

armado, como la carencia de criterios explícitos en cuanto al modo de empleo de este método de combate, implican que el estudio de este marco jurídico, únicamente, podrá realizarse a través de la interpretación analógica.

En esta tarea, son varios los retos que se presentan, por cuanto, en primer lugar, habrá que dirimir el régimen jurídico respecto del que pretende plantearse dicha analogía. Es evidente que el tratamiento que, hasta ahora, han podido recibir otras armas de nueva creación no podrá ser aplicado de forma automática a las armas cibernéticas, pues estas cuentan con unas características que no siempre pueden ser extrapoladas a otro tipo de armamento. Por otra parte, la novedad en el empleo de las mismas, supone la ausencia, como se viene constatando, de un marco normativo de referencia, amén de la carencia de práctica de los Estados. En este sentido, el reto, pues, es de mayor envergadura, por cuanto la observancia de los hechos que con el tiempo se vayan constatando, ofrecerán una visión de la actuación estatal en este ámbito que, por el momento resulta realmente escasa, aunque no inexistente.

Un ejemplo de la práctica estatal más reciente puede encontrarse en la actuación que los Estados Unidos han observado respecto a Corea del Norte, en relación al incidente relativo a la empresa estadounidense Sony. De dicho incidente, hasta la fecha, no se tiene más información que la recogida por los distintos medios de comunicación, por cuanto el mismo no ha podido todavía ser tratado por la doctrina internacionalista. Sin embargo, de la citada información, puede extraerse la conclusión de que el referido "conflicto" ha sido considerado por parte de los Estados Unidos, como un auténtico acto de agresión, de tal modo que, en dicho Estado no hubo dudas en calificar ese ataque cibernético, como una cuestión de "seguridad nacional", mientras se anunciaba una respuesta "proporcionada al ataque sufrido". Como consecuencia de dicho anuncio, diversas sanciones de orden económico fueron acordadas por parte de los Estados Unidos contra Corea del Norte, sin perjuicio de que, además este Estado sufriera varios ciberataques, provenientes de Estados Unidos.[14]

14 Si en un principio, el ataque cibernético sufrido por la empresa Sony, como consecuencia del estreno de una controvertida película, fue considerado una cuestión de *seguridad nacional*,

Este reciente ejemplo de ciberataque pone de manifiesto cómo la práctica de los Estados resultará esencial a la hora de delimitar el régimen jurídico aplicable a los ciberataques, pues dicha práctica será necesaria para consolidación de una costumbre internacional. Pero también revela que en tanto esa práctica no resulte consolidada, es necesario acudir a ese marco legal al que se hacía referencia. En esta labor que se acomete, relativa a la delimitación de dicho marco, resulta esencial destacar una de las características consustanciales a internet, que es la relativa a la posibilidad de doble uso de la red. En virtud de esta consideración, parece conveniente el estudio de la materia desde la perspectiva

---

posteriormente, su valoración fue rebajada a un acto de *vandalismo*. Sin embargo, ello no impidió que se acordaran una serie de medidas por el Gobierno de los Estados Unidos contra Corea del Norte, aun cuando la propia autoría del ciberataque fue cuestionada por empresas privadas del sector. Al respecto, el comunicado de la Casa Blanca, de 2 de enero de 2015, manifestó: "*Today, the President issued an Executive Order (E.O.) authorizing additional sanctions on the Democratic People's Republic of Korea. This E.O. is a response to the Government of North Korea's ongoing provocative, destabilizing, and repressive actions and policies, particularly its destructive and coercive cyber attack on Sony Pictures Entertainment. The E.O. authorizes the Secretary of the Treasury to impose sanctions on individuals and entities associated with the Government of North Korea. We take seriously North Korea's attack that aimed to create destructive financial effects on a U.S. company and to threaten artists and other individuals with the goal of restricting their right to free expression. As the President has said, our response to North Korea's attack against Sony Pictures Entertainment will be proportional, and will take place at a time and in a manner of our choosing. Today's actions are the first aspect of our response*". THE WHITE HOUSE. Office of the Press Secretary. Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea". Disponible en el sitio web: https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s. Fecha de consulta, marzo 2015. Por otra parte, la información de los hechos que se recogió por los medios de comunicación, puede consultarse en los siguientes sitios web: El ataque a Sony fue una venganza de una ex empleada y otros 5 individuos, Internacional EL MUNDO, http://www.elmundo.es/internacional/2014/12/30/54a30537ca4741322b8b457b.html . La secuencia de los hechos acaecidos, puede consultarse en los siguientes medios de comunicación, accesibles a través de los enlaces: "FBI says N Korea behind Sony hacking" Al Jazeera English, http://m.aljazeera.com/story/20141219177312066 90; "FBI blames North Korea for Sony hack" BBC News, http://m.bbc.com/news/world-us-canada-30555997?ns_mchannel=social&ns_campaign=bbc_breaking&ns_source=twitter&ns_linkname=news_central; "Obama vows US response to Sony hack", BBC News, http://m.bbc.com/news/world-us-canada-30555997; "Obama rebaja a "vandalismo" la calificación del "ciberataque" a Sony" Internacional EL MUNDO, http://www.elmundo.es/internacional/2014/12/21/5496c256ca474170238b4574.html; "Las principales páginas web de Corea del Norte, bloqueadas durante varias horas", Internacional EL MUNDO, http://www.elmundo.es/internacional/2014/12/23/5498c6f422601d450b8b4580.html; "North Korea partially back online after internet collapse", BBC News, http://m.bbc.com/news/world-asia-30584093?OCID=twitterasia; "EE UU impone más sanciones a Corea del Norte por el ciberataque a Sony", La Razón digital, http://www.larazon.es/detalle_movil/noticias/8320036/sociedad+tecnologia/ee-uu-impone-mas-sanciones-a-corea-del-norte-por-el-ciberataque-a-sony#.VKfP96MtHqg; "Corea del Norte carga contra EE UU por las nuevas sanciones", Internacional EL PAÍS, http://internacional.elpais.com/internacional/2015/01/04/actualidad/1420392799_630834.html.

de la consideración de internet como arma de doble uso. Es decir, ese amplísimo espectro en las modalidades de uso de internet ya ha sido constatado, desde antiguo, en el empleo de otras armas. Por lo tanto, si, en principio, parece incuestionable el empleo de internet, no resulta extraño, sin embargo, el planteamiento de las condiciones y límites a los que haya de someterse, durante el desarrollo de un conflicto armado.

Las armas de doble uso han recibido a lo largo del tiempo un tratamiento muy diverso por parte del Derecho Internacional. En algunos casos se ha optado por su prohibición a través de instrumentos de carácter convencional, como es el caso de las armas químicas o bacteriológicas. En otros casos, por el contrario, ha sido una nueva interpretación del marco normativo existente, la que ha dado respuesta al uso malicioso de un elemento ya existente. Éste fue el supuesto de las armas nucleares, cuyas limitaciones no fueron recogidas expresamente por el Derecho Internacional Convencional, sino que se desprenden de la Opinión Consultiva de la Corte Internacional de Justicia (en adelante, CIJ), que delimitó los casos en que el armamento nuclear es empleado de modo ilícito.

En cualquier caso, puesto que la aplicación del Derecho Internacional Humanitario (en adelante, DIH) al uso de estas armas será incuestionable, hay que partir de la misma premisa en el caso de los ciberataques. Nuevamente, la naturaleza de este método de combate impone una serie de retos que obligan al estudio de la materia, también aquí, desde una perspectiva teórico- práctica que aporte una visión actualizada de las cuestiones que se abordan. Si únicamente se acometiera el estudio de las cuestiones expuestas desde un plano teórico, a través del examen de la normativa y jurisprudencia internacionales, así como de las principales corrientes doctrinales internacionalistas, difícilmente podría visualizarse la aportación de una respuesta jurídica realmente apropiada. Asimismo, la heterodoxia del elemento cibernético impone un estudio lo más cercano posible a la realidad. A mayor abundamiento, conviene recoger aquí la solución dada al problema de la calificación jurídica de los ciberataques, pues, como ya se puso de manifiesto, la última decisión en esta materia, vendrá de la mano del Consejo de Seguridad de Naciones Unidas. Es decir, que el método de

estudio de casos no puede contemplarse a título meramente ejemplificativo, sino, antes bien, un método de investigación que puede llegar a ser determinante.

Pues bien, sentado lo anterior, procede recoger la definición que se ofrecía al comienzo del presente capítulo considerar en qué medida un ataque informático que se efectúe en el contexto de un conflicto armado (sea éste o no de carácter internacional), en el que se han de observar las normas de DIH, constituye un hecho internacionalmente ilícito del Estado, cometido por acción u omisión[15]. Para que ello sea así, el comportamiento que se atribuye a dicho Estado ha de constituir la violación de una obligación internacional.

Esta expresión denominada "violación de una obligación internacional", abarca tanto las que se hallan contenidas en Tratados como aquéllas que no tienen origen convencional, lo que ha constituido, tradicionalmente, objeto de debate y análisis. Así, siguiendo a PÉREZ GONZALEZ, podemos entender que en la apreciación de "la ilicitud de un acto desde el punto de vista del Derecho Internacional la jurisprudencia internacional suele hablar de «violación de una obligación contraída» por el Estado [16] o de «violación de una obligación impuesta por una norma jurídica internacional», si bien alguna vez se ha referido a un «acto contrario a los derechos» de otro Estado[17].

Sin embargo, como el propio autor hace constar, para un sector doctrinal ha sido preferible la expresión "violación o infracción de una norma de Derecho Internacional", o "violación de una norma o de una obligación jurídico-internacional". La conceptuación definitivamente ofrecida por la Comisión de

15 Comentario 7) al artículo 2 del Proyecto. Comentarios al Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilicitos. Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53º período de sesiones (23 de abril a 1º de junio y 2 de julio a 10 de agosto de 2001). Distribuido inicialmente como Documentos Oficiales de la Asamblea General, quincuagésimo sexto período de sesiones, Suplemento n.° 10. Doc, A/56/10.
16 Permanent Court of International Justice. (1928). *Case concerning the w (claim for indemnity) (merits): documents relating to judgment no. 13 (September 13th, 1928), fourteenth (ordinary) session (1928)*; citado por PÉREZ GONZÁLEZ, M., en *La responsabilidad internacional (I): el hecho internacionalmente ilícito*. DIEZ DE VELASCO, M. Instituciones de Derecho Internacional Público. Tecnos, Madrid, 2013; pp. 843-871, en particular, p. 848.
17 Así se recoge por PÉREZ GONZÁLEZ, M., en *La responsabilidad internacional (I)*, op.cit.; p. 859.

Derecho Internacional, ha sido entendida por MIAJA como «*exigibilidad de una conducta de acción u omisión impuesta por la norma de Derecho*»[18].

La exigencia de responsabilidad internacional al Estado surge, pues, cuando la acción u omisión es atribuible a ese Estado y, además, constituye una obligación internacional contraída por el mismo. De este modo, se analizará aquí, en qué medida puede un ciberataque constituir un hecho ilícito. Desde un punto de vista teórico práctico, se comprobará en qué supuestos un ataque informático puede constituir la violación de una norma de DIH.

Por otra parte, la admisión de la infracción de obligaciones internacionales por omisión tampoco ha planteado tradicionalmente ninguna duda. Tanto la normativa convencional como consuetudinaria, aplicable al caso que se presenta, así lo admiten. También ha sido reconocido así por la Jurisprudencia internacional desde antiguo. No obstante, la novedad del método de combate exige un examen del mismo, a la luz de dichos precedentes, para concluir, a través, nuevamente, del método analógico, concluir en que supuestos ese ilícito internacional, que se derive de una conducta omisiva del Estado, puede generar la responsabilidad internacional del mismo.

2. EL CIBERATAQUE COMO HECHO ILÍCITO INTERNACIONAL. APROXIMACIÓN CONCEPTUAL.

La actividad que pueda desarrollarse a través de internet es capaz ofrecer tan variadas manifestaciones, que resulta necesario, con carácter previo a cualquier otra consideración jurídica, deslindar cuál de ellas es asimilable a un ataque que se podría considerar convencional. De este modo, podrán dejarse al margen todas aquellas actividades informáticas que, sin ser inofensivas, tampoco revisten entidad suficiente para ser consideradas un ataque. Únicamente así podrá vislumbrarse en qué manera los ataques cibernéticos podrán ser utilizados como método de combate y, por lo tanto, derivarse la responsabilidad que a los Estados resulta exigible, como consecuencia de la comisión de un hecho ilícito derivada de su uso. En consecuencia, en los supuestos en que tal asimilación sea

18 Citado por PÉREZ GONZÁLEZ, M., en *La responsabilidad internacional (I)* op.cit; p.860.

posible, será necesario, posteriormente, valorar cuál sea el régimen jurídico aplicable a los mismos, de modo que la cuestión sobre la aplicación del DIH a los ciberataques resulta consustancial.

En este sentido, merece una especial atención la labor desempeñada en esta tarea por determinadas Organizaciones y Organismos Internacionales. De entre todas ellas, cabe resaltar que la función realizada por la Organización del Tratado del Atlántico Norte (en adelante, OTAN) se ha mostrado especialmente relevante al ser, hasta la fecha, la única Organización que ha propiciado la publicación de un Manual en la materia, con cierto ánimo omnicomprensivo en estas cuestiones[19].

El Comité Internacional de la Cruz Roja (en adelante, CIRC) tampoco ha permanecido ajeno a la labor de determinar si, en efecto, la normativa vigente en DIH resulta o no de aplicación a los ciberataques. Desde un primer momento, el CICR dejó sentado que, sin duda alguna, el DIH resulta de aplicación a los nuevos armamentos y tecnologías empleados en la guerra, de conformidad con lo dispuesto en el artículo 36 del Protocolo Adicional I[20] (en adelante, PA I). En palabras de su experta en asuntos legales, el DIH resulta aplicable, en situaciones de conflicto armado, «*cuando las partes recurren a medios y métodos de guerra basados en operaciones cibernéticas*»[21]. La propia esencia del DIH se manifiesta en esta afirmación, llamado a regular los conflictos armados y a dar respuesta, desde este punto de vista, a cualquier novedad fáctica que pueda producirse[22].

19 Como resultado de este interés, en 2013 fue publicado el Manual relativo a Derecho Inteernacional aplicable a la ciberguerra. SCHMITT, M.N. (General Editor). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.

20 Protocolo I Adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales. (BOE de 26 de julio de 1989).

21 Así puede leerse en el documento titulado "*No hay lagunas jurídicas en el ciberespacio*". DROEGE, C., entrevista publicada en la web del CICR en fecha 16 de agosto de 2011. CICR. Disponible en el sitio web: www.icrc.org/ spa/resources/ documents/ interview/2011/cyber-warfare-interview. Fecha de consulta marzo 2013.

22 También se comparte esta opinión en la obra, Un droit dans la guerre?, donde puede leerse: "*L'histoire a d'ailleurs montré que l'apparition de toute réalité factuelle dans une société – qu'elle soit fortement organisée ou non – est concomitante de l'apparition de règles applicables à cette situation. L'applicabilité du droit interne – droit militaire pénal et disciplinaire – aux comportements lors d'un conflit armé, n'a en outre jamais été mise en question. Bien au contraire, les conflits armés, à la différence d'un chaos anarchique, ne peuvent se concevoir sans un minimum de règles uniformément respectées, comme par exemple que les combattants d'une partie puissent tuer ceux de l'autre camp mais pas leurs propres*

No obstante, como acertadamente indicaría SCHMITT, la delimitación de los principales conceptos involucrados en esta nueva situación, de cuya definición depende la aplicación del DIH, quedaba pendiente[23]. En atención a la clasificación de los conflictos que proporciona el DIH resulta interesante, pues, valorar la posibilidad de que los ciberataques se manifiesten en uno u otro, es decir, tanto en un conflicto armado internacional como en un conflicto armado no internacional para, a partir de dicha constatación, entrar a cuestionar si los planteamientos presentes en el DIH resultan aplicables a estos supuestos.

2.1 Estudio de los ciberataques en un conflicto armado internacional.

Partiendo de la premisa de que un conflicto armado, en virtud del DIH, podrá tener el carácter internacional o no internacional, la calificación jurídica de un ataque informático exige comenzar por la noción de conflicto armado internacional que se contiene en el Comentario de los Convenios de Ginebra, que interpreta el artículo 2 común, incluyendo todo desacuerdo entre Estados que conduce a la intervención de las Fuerzas Armadas.

En consecuencia, habrá que comenzar por dirimir si ese ataque informático puede considerarse incluido en la prohibición de la amenaza del "uso de la fuerza" que se establece el artículo 2 de la Carta de Naciones Unidas[24]. Sólo así será posible distinguir aquéllos ataques informáticos que podemos entender constitutivos de un delito cibernético o de una actividad, incluso inofensiva, de aquéllos otros que podrían originar una respuesta armada.

El artículo 2 de la Carta de Naciones Unidas, en su apartado 4, expresamente, establece:

> "Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la

---

commandants ou camarades". SASSÒLI, M., BOUVIER, A., QUINTIN, A. *Un droit dans la guerre? Présentation du droit international humanitaire,* vol. I, Seconde édition. CICR ; p. 4.

23 SCHMITT, M.N., *La guerra de la información: los ataques por vía informática y el ius in bello.* Revista Internacional de la Cruz Roja. 30 de junio de 2002. Disponible en el sitio web: Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/5tecg3.htm. Fecha de consulta marzo 2013.

24 Carta de Naciones Unidas firmada en San Francisco, Estados Unidos, el 26 de junio 1945.

> fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas".

No ha sido necesaria la aparición del elemento cibernético y su posible uso como metodo de combate para constatar las discrepancias en torno al concepto de uso de la fuerza, sino que el mismo ha sido discutido desde antiguo. En su evolución, hay que comenzar citando la Resolución 2625[25] de las Naciones Unidas que, al respecto, proclama, entre otros, el principio de que los Estados, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas. Por otra parte, cuatro años más tarde, la Asamblea General decidió ofrecer una definición de agresión a través de su Resolución 3314[26] en los siguientes términos:

> "el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado o en cualquier otra forma incompatible con la Carta de las Naciones Unidas, tal como se enuncia en la presente Definición".

Sin embargo, no parece que dicha definición aporte demasiada claridad al problema planteado, por cuanto, el principal interrogante sigue sin esclarecerse. Es decir, ¿hasta qué punto la utilización de un ataque informático puede considerarse equivalente al ejercicio de la fuerza armada? o lo que es lo mismo, ¿en qué medida podemos considerar que internet es un arma asimilable a cualquier otra de carácter convencional? Tampoco la enumeración contenida en esta Resolución de los actos que han de considerarse un acto de agresión, con

25 Resolución 2625 (1970), aprobada por la Asamblea General en su 1903ª sesión plenaria, de 24 de octubre 1970. Doc. A/RES/25/2625. Contiene la declaración relativa a los principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los estados de conformidad con la Carta de las Naciones Unidas.

26 Resolución 3314 (1974), aprobada por la Asamblea General en su 2319ª sesión plenaria, de 14 de diciembre de 1974. Doc. RES/3314 (1974).

independencia de la existencia de una declaración de guerra, aporta una solución incontrovertible al tema que aquí se aborda[27].

Tras la Conferencia de Revisión del Estatuto de la Corte Penal Internacional, celebrada en Kampala (Uganda), entre el 31 de mayo y el 11 de junio de 2010, con motivo de la revisión del concepto del crimen de agresión contenido en el referido Estatuto, la definición de "*acto de agresión*", volvió a remitirse a la enumeración presente en la Resolución 3314[28]. De este modo, siguen quedando limitados los actos de agresión a aquellos que, explícitamente, se hallan contenidos en dicha Resolución. Queda, pues, sin resolver si los ciberataques pueden ser conceptuados como acto de agresión, a la luz de las actividades enumeradas en la Resolución, puesto que, en efecto, en una interpretación restrictiva, es evidente que este tipo de ataques no aparecen expresamente citados y, por lo tanto, podrían entenderse excluidos[29].

---

27 La Resolución mencionada entiende que son actos de agresión los enumerados en su artículo 3:

" a) La invasión o el ataque por las fuerzas armadas de un Estado del territorio de otro Estado, o toda ocupación militar, aun temporal que resulte de dicha invasión o ataque, o toda anexión, mediante el uso de la fuerza, del territorio de otro Estado o de parte de él.

b) El bombardeo, por las fuerzas armadas de un Estado del territorio de otro Estado, o el empleo de cualesquiera armas por un Estado contra el territorio de otro Estado.

c) El bloqueo de los puertos o de las costas de un Estado por las fuerzas armadas de otro Estado.

d) El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres navales o aéreas de otro Estado, o contra su flota mercante o aérea.

e) La utilización de fuerzas armadas de un Estado, que se encuentran en el territorio de otro Estado con el acuerdo del Estado receptor, en violación de las condiciones establecidas en el acuerdo o toda prolongación de su presencia en dicho territorio después de terminado el acuerdo.

f) La acción de un Estado que permite que su territorio, que ha puesto a disposición de otro Estado, sea utilizado por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado.

g) El envío por un Estado o en su nombre de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación de dichos actos".

28 Las conclusiones de la citada Conferencia dieron lugar a la Resolución RC/Res.6, aprobada por consenso en la 13ª sesión plenaria el 11 de junio de 2010. Anexo I. Enmiendas al Estatuto de Roma de la Corte Penal Internacional, relativas al crimen de agresión. Doc. RC/Res.6.

29 Así lo entiende, por ejemplo RODRIGUEZ-VILLASANTE, quien excluye lo que denomina "ciberguerra", de la relación de actuaciones contenida en la citada Resolución, entre las que también considera excluidas, el bloqueo de las comunicaciones de un Estado, las demostraciones navales o el despliegue aeronaval en el mar territorial de otro Estado, la denegación de los vuelos militares, en el territorio de otro Estado, el empleo de aviones de combate no tripulados con fines de información, violando las fronteras de otro Estado o la utilización de aeronaves de guerra electrónica operando desde el espacio aéreo internacional. RODRÍGUEZ-VILLASANTE Y PRIETO, J.L. *Nota sobre la Conferencia de revisión del Estatuto de Roma de la Corte Penal Internacional, Kampala (Uganda), 2010*; pp. 3-5. Disponible en el sitio web: http://www.cruzroja.es/dih/pdfs/temas/3_4/3_4.pdf. Fecha de consulta mayo 2014.

Sin embargo, aun partiendo de una interpretación restrictiva, no cabe duda de que los efectos conseguidos por un uso dela fuerza armada convencional, que pretenden evitarse con su tipificación como actos de agresión, también pueden considerarse susceptibles de comisión a través de medios informáticos. Es más, precisamente la conceptuación del ataque informático como acto de fuerza, debería huir de una delimitación estricta, en cuanto a su modo de manifestación y venir circunscrita a los resultados que, con ese ciberataque, puedan producirse. La enumeración contenida en la Resolución 3314 no cita expresamente ningún tipo de arma, hasta ahora conocida, sino que hace referencia a los concretos efectos que cualquiera de ellas podría producir y que pretenden evitarse. Resulta evidente que, por ejemplo, e*l ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres navales o aéreas de otro Estado, o contra su flota mercante o aérea*, prevista en el apartado d), del artículo 3 de la referida Resolución, puede realizarse tanto por medios convencionales como cibernéticos. En consecuencia, será determinante establecer las condiciones para que ese ciberataque pueda ser considerado ataque armado, pues la naturaleza virtual del arma exigirá la concurrencia de una serie de condiciones que, una vez sean constatadas, nada podrá impedir que ese ataque cibernético esté prohibido, de conformidad con lo establecido en la Resolución 3314.

La interpretación restrictiva que proponen algunos autores, en efecto, limita las capacidades del Consejo de Seguridad de Naciones Unidas a la hora de determinar, en qué momento una actuación puede calificarse como acto de agresión, en virtud de la competencia que le atribuye el artículo 4 de la misma Resolución. No obstante, pese a los inconvenientes que ello pudiera originar, en el ámbito político, no parece del todo indeseable esta última opción, por cuanto permitiría una mejor adaptación del Derecho Internacional a las nuevas modalidades de los conflictos armados y al empleo de armamento de vanguardia.

La propia Resolución ofrece una serie de criterios moduladores de este concepto. De este modo, se entiende que para que el acto de agresión pueda ser calificado como "*crimen de agresión*" y, por lo tanto, el Tribunal Penal Internacional (en adelante, TPI) pueda ejercer su competencia, el mismo ha de ser

un acto de agresión que "*por sus características, gravedad y escala constituya una violación manifiesta de la Carta de las Naciones Unidas*". De este modo, como acertadamente concluye QUESADA ALCALÁ, se consigue que, únicamente, cuando los usos prohibidos por el Derecho Internacional, alcanzan el umbral pertinente, los hechos cometidos sean competencia del TPI[30]. Todo ello redunda en el hecho de que la "*agresión*", como indica CLARK, sea interpretada como

> "la más grave y peligrosa forma del uso de la fuerza y por lo tanto, determinar si la misma se ha cometido, requiere la consideración de todas las circunstancias relativas a cada caso concreto, incluyendo la gravedad de los hechos y sus consecuencias, caso por caso, de acuerdo con la Carta de Naciones Unidas"[31].

Por otra parte, mantener la enumeración de resultados prevista por la Resolución 3314 aporta la ventaja de contar con una serie de actos que, por su consenso entre los Estados, pueden ser calificados, sin discusión, como "*actos de agresión*"; cuestión ésta de vital importancia, si retomamos la idea de que éstos han de limitarse a los más graves en el ámbito internacional[32].

Por último, dicha interpretación, además, resulta avalada por la que se ha realizado en el ámbito jurisprudencial, pues estos criterios ya han sido tenidos en cuenta por la CIJ, al calificar determinadas actuaciones, como las llevadas a cabo por parte de Uganda en el territorio del Congo. Para la Corte, la intervención militar de Uganda resultó de tal "*magnitud y duración*" que constituyó una grave violación de la prohibición contenida en el artículo 2 de la Carta de Naciones Unidas y, al respecto estableció que:

---

30 QUESADA ALCALÁ, C., *El crimen de agresión como amenaza a la seguridad global. La respuesta del Derecho Internacional a los problemas actuales de la seguridad global*. Cuadernos de Estrategia. Número 160. Instituto Español de Estudios Estratégicos. Cruz Roja Española-Centro de Estudios de Derecho Internacional Humanitario. Enero 2013; pp 88- 92.

31 CLARK, R. S. *Amendments to the Rome Statute of the International Criminal Court Considered at the first Review Conference on the Court, Kampala, 31 May-11 June 2010*. Goettingen Journal of International Law, vol. 2, no. 2 (2010); 689-711, en particular, p.711. "*The achievement of consensus on the crime of aggression, activating the Court's jurisdiction – albeit with some delay – constituted a remarkable achievement and a great source of satisfaction to those who have laboured for it these many years*".

32 HEINSCH, R. *The Crime of Aggression After Kampala: Success or Burden for the Future?* Goettingen Journal of International Law 2, 2010; pp. 713-743, en particular, p.725: "*the members of the Special Working Group were obviously determined to use a definition which has at least some support on the international level*."

> "In relation to the first of the DRC's final submissions, the Court accordingly concludes that Uganda has violated the sovereignty and also the territorial integrity of the DRC. Uganda's actions equally constituted an interference in the internal affairs of the DRC and in the civil war there raging. The unlawful military intervention by Uganda was of such a magnitude and duration that the Court considers it to be a grave violation of the prohibition on the use of force expressed in Article 2, paragraph 4, of the Charter".[33]

En cualquier caso, hay que tener siempre presente que la prohibición del uso de la fuerza constituye una norma de aplicación universal, toda vez que se trata de Derecho consuetudinario aplicable, por lo tanto, a cualquier Estado, salvo objeción persistente[34].

En esta labor de indagación dirigida a discernir si los ciberataques pueden constituir o no un ataque armado, también es preciso acudir a la doctrina internacionalista que, a lo largo del tiempo ha ofrecido múltiples criterios interpretativos, para determinar si un ataque puede ser contemplado, dentro de la definición de agresión, ofrecida por Naciones Unidas. Entre ellos, cobra fuerza la teoría interpretativa basada en los resultados[35]. Abandonando, así, el tradicional método de determinar la existencia del uso de la fuerza, basado en la naturaleza del ataque, se aboga por considerar los efectos que pueda tener un ataque cibernético para, de este modo, determinar la adecuación del mismo al Derecho Internacional. La teoría que se fundamenta en la naturaleza del ataque no puede resultar completamente adecuada en este caso, por cuanto nos encontramos con un tipo de amenazas que no responden, de forma idéntica, a la naturaleza de las amenazas hasta ahora conocidas. Es más, puede considerarse que dicha diferencia ha motivado un cambio en la propia concepción de los

33 Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005; par. 164.

34 Así queda establecido en la Sentencia relativa al asunto Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986; par. 209.

35 Este es el criterio interpretativo que expone RABOIN, B. *Corresponding Evolution: International Law and the Emergence of Cyber Warfare.* Cleveland State Law Review, no. 31, 2013; pp. 603-668.

conflictos, que incluyen el elemento cibernético, como una parte esencial en el desarrollo de los conflictos convencionales.[36]

Es evidente, por otra parte, que determinados ciberataques son susceptibles de causar un daño efectivo, real y equiparable al que podría suponer el empleo de la fuerza cinética[37]. No obstante, los ataques informáticos que, hasta ahora, han provocado mayor alarma en la Comunidad Internacional, ofrecen dudas, en cuanto a su definición como ataques armados o uso de la fuerza. Además, teniendo en consideración el contexto en el que algunos de ellos se han producido, no es arriesgado aventurar que podrían haber originado una respuesta, por parte del Estado víctima de los mismos, que, a su vez, habría constituido otra contravención al Derecho Internacional. Esta situación es la que se produjo en los ataques recibidos por Ucrania, durante el conflicto interno, sufrido desde el invierno de 2014, así como en el desarrollo de las tensiones diplomáticas con Rusia[38]. En semejante contexto, no parece extraño que Ucrania hubiera interpretado el lanzamiento de ciberataques como un acto de agresión.

No hay que olvidar, por otra parte, que la enumeración de los actos de agresión contenida en el artículo 3 de la Resolución 3314 no es de carácter exhaustivo, sino que queda supeditada a la decisión del Consejo de Seguridad de Naciones Unidas que tendrá que determinar, en cada caso, qué otros actos constituyen agresión con arreglo a las disposiciones de la Carta. Pues bien, en el

---

36 En este sentido se expresó, en julio de 2011, el Departamento de Defensa de los Estados Unidos, al publicar la Estrategia para las Operaciones en el Ciberespacio, documento que parte de la base de que la Seguridad Nacional ha de ser redefinida a través del concepto de ciberespacio y que, tanto las operaciones militares, como las de Inteligencia y las comerciales dependen del ciberespacio para ser realizadas con éxito; *Strategy for Operating in Cyberspace, Department of the Army*, 2011 en: www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/ResenaEstrategiaoperacionesCiberespacio_julio2011.pdf. Fecha de consulta, junio de 2014.

37 RABOIN, B., *Corresponding Evolution: International*, op.cit; p. 604.

38 En relación a estos ataques, puede consultarse STINISSEN, J. A., *Legal Framework for Cyber Operations in Ukraine*. Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO Cooperative Cyber Defense Centre Of Excellence Publications, Tallin 2015; pp. 123-134. De los mismos hechos ha dado cuenta la prensa internacional, pudiendo consultarse, en este sentido, la página web www.bbc.com, cuya publicación digital, de 5 de marzo de 2014, refería los ataques producidos afirmando: "*Security forces in Ukraine have accused the Russian army of disrupting mobile communications. Smaller-scale attacks have seen news websites and social media defaced with propaganda messages*". http://www.bbc.com/news/technology-26447200. Fecha de consulta marzo 2014.

referido supuesto de los ataques cibernéticos sufridos por Ucrania no se ha producido dicho pronunciamiento, como tampoco en relación a otros que ya habían sido constatados con anterioridad en el tiempo, en similar contexto[39]. No obstante, en atención a los criterios interpretativos expuestos y teniendo en cuenta los efectos, de los que se tiene conocimiento, sufridos por Ucrania, no parece que estos ciberataques constituyan un ataque de la envergadura suficiente para tener la consideración de "uso de la fuerza" o "ataque armado".

El concepto de uso de la fuerza ha sido también estudiado por la doctrina desde una perspectiva, que implica el análisis de los conceptos de violencia armada, fuerza coercitiva o fuerza de interferencia[40]. Desde este punto de vista, se entiende que sólo la fuerza física armada queda prohibida por el artículo 2 (4) de la Carta de Naciones Unidas y que la definición de ataque armado es mucho más restrictiva que la de uso de la fuerza, utilizada por la Carta de Naciones Unidas. En consecuencia, puede haber actos que violen la prohibición del artículo 2(4) y que, sin embargo, no constituyan un ataque armado tal como hace constar De LUCCA, quien entiende avalada tal postura por la Jurisprudencia de la CIJ[41]. Siguiendo la presente construcción teórica que propone un criterio interpretativo como el expuesto, cabe plantearse las consecuencias prácticas de su aplicación. Así, si el artículo 2 (4) de la Carta prohíbe, exclusivamente, el uso de la fuerza

39 De entre todos los ciberataques de los que a diario se tiene conocimiento, han sido los sufridos por Georgia en el año 2008, los que han sido objeto de una atención especializada, de nuevo por parte de OTAN, que ha publicado, al respecto la obra. TIKK, E. KASKA, K., RÜNNIMERI, K., KERT, M., TALIHÄRM, A.-M., VIHUL, L. Cyber Attacks Against Georgia: Legal Lessons Identified. NATO Cooperative Cyber Defense Centre Of Excellence Publications, Tallin 2008.

40 DE LUCCA, C.D., *The Need for International Laws of War to Include Cyber Attacks Involving State and Non- State Actors*. Pace International Law Review Online Companion. School of Law, Vol. 3:9, enero 2013; p. 278-315, en particular; p.294.

41 En este sentido, el autor, con base en el fallo de la CIJ, en relación con las Actividades Militares y Paramilitares en y contra Nicaragua, argumenta que, "*It is also widely understood that the definition of "armed attack" is much narrower than the definition of "force" under the U.N. Charter. For example, there may be acts that violate Article 2(4)'s prohibition on the use or threat of force, but do not constitute an "armed attack*." El pronunciamiento de la CIJ citado por DE LUCCA es el siguiente: "*[A]n armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by… a State of armed bands…which carry out acts of armed force against another State…" The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather tan as a mere frontier incident had it been carried out by regular armed forces. According to the ICJ, armed attacks are those that constitute the "most grave forms of the use of force*." DE LUCCA, C.D., *The Need for International*, op.cit; p. 295.

física, el lanzamiento del virus Stuxnet no resultaría recogido dentro de la prohibición[42]. Es decir, en coherencia con este criterio, la introducción del virus Stuxnet, por ejemplo, no podría ser considerada como un acto de fuerza, por cuanto las centrales nucleares de Irán, en ningún momento, fueron atacadas por la fuerza física y tampoco puede concluirse que fuera un ataque armado, según la definición dada más arriba, en tanto que no parece la forma más grave de uso de la fuerza.

El controvertido lanzamiento de este virus también puede servir de ejemplo para revelar la dificultad de la conceptuación, no sólo de este supuesto, sino de los ataques informáticos, en general. Si incluimos en esta labor interpretativa, un criterio adicional, podría examinarse el ataque por el virus Stuxnet, a la luz de la teoría que aúna los criterios relativos a la instrumentalidad del ataque, el objetivo de dicho ataque y las consecuencias del mismo[43]. De esta forma, en función del criterio de la instrumentalidad, un ciberataque no constituye un ataque armado de acuerdo con el artículo 2(4) toda vez que carece de las características físicas que, tradicionalmente, han sido asociadas a los ataques militares.

---

42 Son muchos los autores que han prestado atención a este ciberincidente, que ha sido definido como: "(…) *start of a new era in the arms-race in cyber security. First time in history, a targeted cyber attack was discovered that aimed at physically destroying part of the critical infrastructure of a state*". Así se expresan BENCSATH B., et al. *The Cousins of Stuxnet: Duqu, Flame, and Gauss*. Future Internet (núm.4, 2012) ; pp. 971-1003. Disponible en www.mdpi.com/journal/futureinternet-04-00971.pdf. Acceso noviembre 2013: "*Like other computer worms, Stuxnet spread indiscriminately from one vulnerable computer to the next. What set it apart from the thousands of other worms that went before it is that it was designed to unleash its payload only when it entered an industrial control system (ICS) matching the characteristics of Iran's nuclear enrichment facility at Natanz. And when it did, it tampered with the code of the programmable logic controller (PLC) used to control the centrifuges at Natanz, ultimately destroying about a thousand centrifuges and disrupting Iran's nuclear program. No previously reported worm had done anything like that before, either in terms of precision targeting or causing physical damage through ICS manipulation*". También al respecto, puede consultarse DENNING, D. E. *Stuxnet: What Has Changed? Future Internet* 2012, 4; pp 672-687. Disponible en el sitio web: http://www.mdpi.com/1999-5903/4/3/672. Fecha consulta octubre 2013. Por su parte, el Manual de Tallin, define Stuxnet como "*A computer worm that was designed to target software and equipment comprising Siemens Corporation developed Supervisory Control and Data Acquisition (SCADA) systems. The payload of the Stuxnet malware included a programmable logic controller rootkit. Stuxnet came to light after it was discovered that it had been used to target Iranian facilities at which Siemens SCADA systems are used to control centrifuges involved in the enrichment of uranium*". SCHMITT, M.N. (General Editor). Tallin Manual, op.cit; p. 214.

43 Este es el criterio propuesto por HOLLIS. Al respecto, puede consultarse, HOLLIS, D.B., *Why States Need an International Law for Information Operations*. Lewis & Clark Law Review, vol. 11. 2007, Temple University Legal Studies Research Paper no. 2008-43; pp. 1023-1061.

Para HOLLIS, la Carta de las Naciones Unidas ofrece cierto apoyo a esta visión, por cuanto, su artículo 41, al enunciar las medidas que no involucran el uso de fuerza armada, incluye las "*interrupciones completas o parciales de telegrafía, radio, y otros medios de comunicación*"[44]. Sin embargo, aun cuando se pretenda abogar por una interpretación basada en criterios restrictivos, no puede contemplarse la anterior teoría como una fórmula adecuada a la naturaleza y gravedad de las situaciones a las que, con toda seguridad, la Comunidad Internacional deberá hacer frente en un futuro. Excluir los ataques informáticos del concepto de ataque armado, por el mero hecho de no compartir las características físicas de los ataques militares, conocidos hasta ahora, y por la exclusión conceptual, realizada por el artículo 41 de la Carta, implicaría, a buen seguro, un agravamiento de la situación jurídica actual. Por otra parte, la interpretación expuesta en relación al contenido del artículo 41, tampoco resulta viable en este ámbito por cuanto, en la actualidad, internet no puede ser considerado, exclusivamente, como un medio de comunicación, una vez que ha quedado sobradamente demostrado que sus capacidades son infinitamente mayores.

Si, dentro de esta conjunción de criterios analizamos el objetivo del ataque, resulta que, por ejemplo, un ciberataque constituirá uso de la fuerza, siempre que penetre en las llamadas infraestructuras críticas de un Estado, incluso, cuando no cause daños físicos. Sin perjuicio del estudio de los ciberataques relacionados con las infraestructuras críticas que se abordará en un Capítulo posterior, en esta fase del estudio puede afirmarse que esta construcción teórica presenta el problema de ser excesivamente amplia, por cuanto los efectos de un ciberataque pueden abarcar, como se ha expresado anteriormente, un gran rango de actividades: desde mera propaganda a actividades potencialmente peligrosas, incluso, destructivas. En efecto, en aplicación de este criterio, un ciberataque dirigido a infraestructuras críticas, como lo fue el caso de Stuxnet, podría resultar incluido

44 HOLLIS, D.B., *Why States Need*, op.cit; p.1041.

dentro del concepto de uso de la fuerza, pero también lo estarían aquéllos que resultaran netamente inoperantes o inofensivos.

Si, por otro lado, se atiende al criterio que propone tomar en consideración las ocasionales consecuencias de un ataque cibernético, puede concluirse que un ciberataque constituirá uso de la fuerza, siempre que su pretensión sea causar los mismos efectos, que podría generar un ataque producido por fuerza cinética. En el repetido caso de la introducción del virus Stuxnet en la central nuclear iraní, no cabe duda de que sus efectos, *a priori*, se concretaron en la neutralización del desarrollo del enriquecimiento de uranio por el Estado aludido[45]; resultado éste que, en efecto, podría asimilarse al obtenido en el uso de otro tipo de armas.

Aun de forma breve, no puede dejar de mencionarse que la construcción teórica relativa a la prohibición del uso de la fuerza, necesariamente, ha de complementarse con el Derecho Consuetudinario que establece la prohibición de los Estados de intervenir en los asuntos internos de otros Estados. Así quedó establecido en la sentencia de la Corte Internacional de Justicia en el caso de las Actividades Militares y Paramilitares en y contra Nicaragua, al determinar la CIJ que, en los supuestos en que la injerencia tomara forma de uso o amenaza de la fuerza, el Derecho consuetudinario de no intervención resulta colindante con el artículo 2 (4) de la Carta de Naciones Unidas[46].

Como se analizará con mayor precisión más adelante, es innegable, por último, que el uso de la fuerza, utilizado en respuesta a un ciberataque deberá cumplir con los principios de necesidad y proporcionalidad establecidos, asimismo, por la legalidad internacional, así como con el resto de las normas relativas a la conducción de hostilidades[47].

---

45 Al respecto, vease asimismo BENCSATH B., et al. *The Cousins of Stuxnet*, op.cit.; y DENNING, D. E. *Stuxnet: What Has Changed*? op.cit.; pp 672-687, así como SCHMITT, M.N. (General Editor). Tallin Manual, op.cit.; p. 214.

46 La CIJ, en su Sentencia Military and Paramilitary Activities in and Against Nicaragua, al respecto, afirma que, "*The Court therefore finds that no such general right of intervention, in support of an opposition within another State, exists in contemporary international law. The Court concludes that acts constituting a breach of the customary principle of non-intervention will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations*". Military and Paramilitary Activities in and Against Nicaragua, doc. cit,; par. 209.

47Así se expresan HATHAWAY, O. A. y otros. *The law of cyber-attack*. Yale Faculty Scholarship Series, paper 3852, 2012; pp. 817- 886.

La delimitación conceptual de los ciberataques ha sido, asimismo, abordada por las principales Organizaciones Regionales de las que España forma parte. Con carácter primordial, procede aquí realizar una exposición de las valoraciones que, al respecto, se han ofrecido por la OTAN y por la Unión Europea (en adelante, UE), habida cuenta los compromisos a los que España podría tener que hacer frente, en el fututo, en relación con posibles ciberataques.

2.1.1. La delimitación conceptual de los ciberataques en el ámbito de la OTAN.

En consonancia con lo expuesto hasta ahora y teniendo en cuenta la pertenencia de España a la OTAN, resulta preciso hacer una específica mención al Tratado del Atlántico Norte, en la idea de que la labor que desempeñe esta Organización, en el futuro, puede ser crucial, pues la conceptuación de los ciberataques como ataques armados será determinante en los supuestos en que a la misma se le plantee una futura intervención.

Sin perjuicio del análisis que se realizará del artículo 5 del Tratado de la OTAN, cuando se atiendan las cuestiones relativas a la legítima defensa, a los efectos que atañen al concepto de ataque, hay que hacer constar aquí que este artículo arroja escasa luz.

Como se verá, el Tratado no aporta un concepto de un ataque armado, sino que se limita a establecer que, una vez producido contra cualquiera de los Estados Parte, podrá activarse el ejercicio del derecho de legítima defensa colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas. La OTAN, por lo tanto, circunscribe la aplicación del Tratado a que el ataque se produzca en un determinado ámbito territorial. Sin embargo, en este sentido, hay que poner de relieve que, al igual que hubo de ser superada la delimitación que considera posible el desarrollo del conflicto bélico en el espacio terrestre, marítimo y aéreo, para extenderlo al espacio ultraterrestre, debería tenerse en

cuenta, en estos momentos, la posibilidad de que los conflictos sean librados en un ámbito virtual y no físico, tal y como indica GÓMEZ DE ÁGREDA[48].

La Cumbre de la OTAN, celebrada en Gales en septiembre de 2014, sintetizó la postura de la Organización en relación a esta materia. Sin llegar a profundizar en el concepto de ciberataque, desde un punto de vista jurídico, pues no parecía ésta una tarea propia de la naturaleza de la Cumbre, lo cierto es que las conclusiones alcanzadas en materia de ciberdefensa, resultan en cierto modo esclarecedoras. Así, se afirma por parte de la OTAN que, el Derecho Internacional, en el que queda incluido obviamente el DIH, así como la Carta de naciones Unidas, son de aplicación en el ciberespacio. Esta indubitada aplicación se justifica en la apreciación de los ciberataques como actividades que pueden amenazar a la prosperidad, seguridad y estabilidad euroatlánticas y cuyo impacto puede llegar a ser tan dañino para las sociedades modernas como el ocasionado por un ataque convencional[49]. Con posterioridad, la Cumbre celebrada en Varsovia, en agosto de 2016, volvió a tratar el asunto, al considerar la diversa naturaleza que pueden presentar las amenazas a su seguridad, afirmando al respecto que "*The Alliance faces a range of security challenges and threats that originate both from the east and from the south; from state and non-state actors; from military forces and from terrorist, cyber, or hybrid attacks*[50]", reconociendo, en relación con el elemento cibernetico que "*cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea*[51]".

48 En este sentido, puede consultarse GÓMEZ DE AGREDA, A. *El ciberespacio como escenario del conflicto. Identificación de las amenazas*. El Ciberespacio nuevo escenario de confrontación. Monografías CESEDEN, núm. 126. Febrero 2012; pp. 169 a 203, en particular, p. 171.

49 El aludido documento es *Wales Summit Declaration.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales"; par. 72.

50 La citada Cumbre tuvo como resultado el documento: Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016; par. 5. Asimismo, en relación a las conclusiones alcanzadas en la Cumbre de Varsovia, puede consultarse, el articulo de MOLINER GONZALEZ, J. *La cumbre de la OTAN en Varsovia.* Documento de Opinion 79bis/2016, de 2 de agosto de 2016. Instituto Español de Estudios Estrategicos. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO79bis-2016_CumbreOTAN_Varsovia_Moliner.pdf. Fecha de consulta septiembre de 2016.

51 Warsaw Summit Communiqué; doc.cit.; par.70.

Al margen de otras consideraciones, que pudieran ser de carácter político[52] en lo que aquí atañe, resulta relevante la determinación de la organización en la aplicación del DIH a los ciberataques, así como la apreciación recogida en cuanto a su equivalencia destructora con otras armas convencionales. De forma evidente, en este planteamiento se hace necesario, de nuevo, concretar en qué casos el concepto de ataque armado puede identificarse con los ataques cibernéticos, a los efectos de aplicar el artículo 5 del Tratado. Pues bien, en esta materia, la OTAN renuncia, al menos, a través de esta Declaración institucional, a ofrecer una definición o elenco de criterios aplicables, con carácter general y remite la cuestión a lo que, en cada supuesto, decida el Consejo del Atlántico Norte, es decir el órgano máximo de representación y decisión de la Organización[53]. No parece, sin embargo, criticable esta postura. Al contrario, puede decirse que la misma es coherente con el sistema previsto en la Resolución 3314 de la Asamblea General de las Naciones Unidas que, en último término, deja en manos del Consejo de Seguridad la calificación de los hechos. Si bien es cierto que, una ausencia de definición en este ámbito constituye una laguna jurídica, nunca deseable, no lo es menos que, en tanto no haya consenso al respecto, la delimitación de los casos por el máximo órgano de la Organización de Naciones Unidas y de la OTAN, parece una solución oportuna[54].

En este punto, resulta necesario hacer notar también que la OTAN ha sido, sin duda, una de las Organizaciones que mayor actividad ha desarrollado en la

52 Estas consideraciones pueden ser consultadas en el Documento Informativo elaborado por Ramírez Morán, publicado por el Instituto Español de Estudios Estratégicos. RAMÍREZ MORÁN, D. *La ciberdefensa en la Cumbre de Gales de la OTAN*. 13/2014, de 15 de octubre de 2014. Disponible en el sitio web web:http://www.ieee.es/Galerias/fichero/docs_informativos/2014/DIEEEI13-2014_Ciberseguridad_CumbreGales_DRM.pdf. Fecha de consulta enero 2015.

53 Así se recoge en el artículo 9 del Tratado del Atlántico Norte, firmado en Washington D.C., el 4 de abril de 1949.

54 En consonancia con esta conclusión puede consultarse asimismo la reflexión que, sobre el uso de la fuerza por las Naciones Unidas, realiza DOMENECH OLMEDAS, para quien: "*La eficacia del sistema mundial de seguridad colectiva, depende no solo de la legalidad de lasdecisiones, sino de que haya una idea común de que son legitimas y de que se adoptan sobre la base de pruebas sólidas y por buenas razones, tanto morales como jurídicas*". DOMENECH OLMEDAS, J.L., *La acción militar en las operaciones de paz*. Estudios de Derecho Internacional y de Derecho europeo en homenaje al Profesor Manuel Pérez González. Tomo I. Aznar Gómez, M., (Coordinador). Tirant lo Blanch. Valencia, 2012; pp. 441-489, en particular, p. 444.

investigación científica en la materia que ahora nos ocupa; hecho éste que no puede resultar extraño, habida cuenta la naturaleza de la propia Organización, así como el número de ciberataques sufridos por alguno de sus Estados miembros y aun por su propia página web[55].

En la tarea dirigida a lograr una calificación jurídica de los ciberataques, no pueden desatenderse las consideraciones realizadas por el Manual de Tallin, pues, aunque el mismo no constituye la doctrina oficial de la OTAN, es cierto que la labor realizada por sus autores, en este ámbito, puede ser tenida como una referencia de utilidad en ciertos aspectos. En este caso, el Manual considera que una ciberoperación constituirá uso de la fuerza, cuando ello resulte de la combinación de, al menos, siete factores, que son enumerados y someramente explicados en la Norma 11 de la citada obra[56]. Dichos factores son: la severidad del ataque; su inmediación; el efecto directo causado; la invasividad; la posibilidad de medir sus efectos; el carácter militar de dicho ataque y la posible implicación, en el mismo, de un Estado. Se propone, pues, por parte de los autores del Manual de Tallin, un análisis de los ataques cibernéticos basado en la conjunción de estos criterios que, a su juicio, permitirá determinar si el mismo constituye un ataque armado[57]. Así, esa aplicación conjunta de los referidos criterios parece abogar por una perspectiva restrictiva que, sin duda, permitirá descartar, de la inclusión en el concepto de uso de fuerza, aquellos ciberataques de menor entidad. Desde este punto de vista, aun teniendo en cuenta las prevenciones realizadas, por los autores de la obra, relativas a la necesidad de

55 Estos ataques fueron constatados una vez la OTAN se manifestó contraria a la actividad de Rusia en relación a Ucrania. La web oficial de la OTAN incluyó un vídeo en el que expresaba su postura en dicho conflicto. De tales ataques informó la prensa internacional, en fecha 16 de marzo de 2014, tal como puede consultarse http://es.reuters.com/article/topNews/idESMAEA2F00620140316.

56 SCHMITT, M.N., (General Editor). Tallin Manual, op.cit.; pp. 45- 52.

57Estos mismos criterios habían sido ya propuestos por SCHMITT, M.N., *Cyber operations and the jus ad bellum revisited.* Villanova Law Review, vol. 56, diciembre 2011; pp. 569- 606 y, posteriormente, recogidos por FOLTZ A.C., *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force! Debate. JFQ,* issue 67, 4th quarter 2012; pp. 40-48. También han sido realizadas dichas consideraciones por ZIOLKOWSKI K., *Ius ad bellum in "Cyberspace – Some Thoughts on the "Schmitt- Criteria" for Use of Force.* CZOSSECK, C. y otros, 2012 4th International Conference on Cyber Conflict, NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn, 2012.

contextualizar los ciberataques, no parece generar dudas la categorización del virus Stuxnet, como una materialización del uso de la fuerza. No puede concluirse de la misma forma, sin embargo, respecto a los ataques sufridos por la OTAN en su página web que, difícilmente, podrían verse encuadrados en algunos de los criterios expuestos, tales como la severidad de los mismos o su carácter militar.

Esta tesis restrictiva responde, de forma más fiel, a la legalidad internacional que ha sido examinada y, a pesar de su complejidad, la aplicación de la misma resulta más deseable que la del resto de los criterios doctrinales expuestos a lo largo del presente estudio. A mayor abundamiento, también parece responder a los límites que han de atribuirse al concepto de acto de agresión para ser considerado crimen de agresión, en consonancia con la definición adoptada en la Cumbre de Kampala.

En consecuencia, en tanto no se cuente con una definición de uso de la fuerza, que comprenda, taxativamente, los supuestos en que los ciberataques han de ser incluidos, convendría atender a esta última tesis propuesta por el Manual de Tallin, a la hora de determinar los recursos y medios que han de ponerse a disposición de la Defensa Nacional. Es decir, los medios que, en un momento dado, tendrán que activarse para hacer frente a los conflictos armados, que se puedan desencadenar en la defensa de los intereses o valores nacionales y de los que se comparten con los Estados aliados, en virtud de nuestra pertenencia a las Naciones Unidas, la OTAN y la Unión Europea[58].

2.1.2. La delimitación conceptual de los ciberataques en el ámbito de la UE.

En el ámbito de la Unión Europea (en adelante, UE) resulta obligada la mención a la llamada "clásula de asistencia mutua" pues constituye una referencia singular contenida en el apartado 1) del artículo 42 del Tratado de la Unión Europea (en adelante, TUE). El mismo especifica que la Política Común de

58 Así se prevé en la Estrategia Española de Seguridad Nacional. *Estrategia de Seguridad Nacional. Un Proyecto Compartido*, Presidencia del Gobierno, 2013.

Seguridad y Defensa (en adelante, PESD) forma parte integrante de la Política Exterior y de Seguridad Común. Según el apartado primero de este artículo, esta política común,

> "ofrecerá a la Unión una capacidad operativa basada en medios civiles y militares. La Unión podrá recurrir a dichos medios en misiones fuera de la Unión que tengan por objetivo garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la Carta de las Naciones Unidas".

Son varias las consecuencias que se derivan de esta previsión en el TUE y de su contenido, pues supone una novedad en determinados aspectos, en relación con las disposiciones del Tratado de la OTAN. De esta manera, nos encontramos con que, a pesar de no tratarse de una Organización Regional de índole militar, a la luz del artículo 42 del TUE, puede hablarse de una capacidad operativa que incluye medios militares.

En la misma línea, el apartado 7 de dicho artículo contempla que los Estados miembros se comprometen a "*prestar ayuda y asistencia, con todos los medios a su alcance y de conformidad con el artículo 51 de la Carta de las Naciones Unidas, a cualquier otro Estado miembro objeto de una agresión armada en su territorio*".

Las consecuencias que dicha previsión pudiera tener, a la hora de ejercer la legítima defensa colectiva por parte de los Estados miembros de la UE, serán tratadas al examinar dichas cuestiones en el capítulo quinto. Sin embargo, parece oportuno atender, aunque sea someramente, al contenido de esta cláusula, con el objeto de analizar la noción de ataque armado en la que se basa esta asistencia mutua.

La remisión expresa a la Carta de Naciones Unidas, en los apartados 1) y 7) del artículo 42 TUE indica, no solo el lógico sometimiento de la UE a la Carta sino, también la ausencia de un concepto propio, tanto de ataque armado como de legitima defensa. En efecto, el TUE no realiza ninguna aportación conceptual en este aspecto, pese a haber incorporado una claúsula, que pudiera haberlo requerido. De hecho, el Protocolo sobre la cooperación estructurada permanente,

establecida por el artículo 42 del TUE[59], alude expresamente a la pertenencia a la OTAN de algunos de los Estados miembros de la UE, de forma que parece que esta asistencia mutua podría entenderse satisfecha a través de los mecanismos incorporados en el Tratado OTAN. Por lo tanto, esta cláusula podría parecer redundante, desde un punto de vista práctico, tenendo en cuenta que, además, no realiza ninguna innovación conceptual al respecto.

En consecuencia, la activación de dicha cláusula de asistencia mutua se justificará, únicamente, en los supuestos en que se produzca un ataque armado, en los términos que hemos visto. En una primera aproximación, parece que esta posibilidad podría ofrecer una mayor seguridad jurídica. Sin embargo, cuando se ha producido la activación de la claúsula de asistencia mutua ha suscitado críticas entre la doctrina internacionalista motivadas, precisamente, por la naturaleza jurídica de los hechos, a los que se ha pretendido dar respuesta[60].

En efecto, la invocación de este artículo 42.7 con el objetivo de hacer frente a actos terroristas ha supuesto un factor de incertidumbre jurídica, en relación al acto de agresión al que se puede dar respuesta en legítima defensa. No obstante, es digno de mención el hecho de que, tras la activación de esta cláusula, se ha contado con la correspondiene decisión de Naciones Unidas, de tal forma que, aunque pudiera ser discutido el concepto de ataque que se manejó en ese

59 El Protocolo (n. 10) sobre la cooperación estructurada permanente establecida por el artículo 42 del tratado de la Unión Europea recuerda " *que la política común de seguridad y defensa de la Unión respeta las obligaciones derivadas del Tratado del Atlántico Norte para los Estados miembros que consideran que su defensa común se realiza dentro de la Organización del Tratado del Atlántico Norte, que sigue siendo el fundamento de la defensa colectiva de sus miembros, y que es compatible con la política común de seguridad y defensa establecida en este marco*". Este documento, así como un estudio detallado de las cuestiones relativas a la posibilidad de creación de unas Fuerzas Armadas europeas, pueden consultarse en la obra, AA.VV. *El proceso hacia unas fuerzas armadas europeas: realizaciones y desafíos*. Documentos de Seguridad y Defensa, núm. 55. Escuela de Altos Estudios de la Defensa, Ministerio de Defensa, marzo 2013; p. 101.

60 En este sentido, véase GONZALEZ ALONSO, L.N., *¿Daños jurídicos colaterales? La invocación del artículo 42.7 del Tratado de la Unión Europea y la lucha contra el terrorismo internacional*. Documento disponible en http://www.reei.org/index.php/revista/num32/archivos/07_Estudio_GONZALEZ_LuisN.pdf. Fecha de consulta enero 2017 y ARTEAGA, F. *La solidaridad española con Francia y el artículo 42.7 del Tratado de la UE. Real Instituto Elcano*. ARI 69/2015, de 23 de noviembre de 2015. Documento disponible en el sitio web: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/ari69-2015-arteaga-la-solidaridad-espanola-con-francia-articulo-427-tratado-ue. Fecha de consulta enero de 2016.

momento, no fue una elaboración conceptual de la UE La Resolución del Consejo de Seguridad de las Naciones Unidas 2249 (2015) [61] avaló la intervención instada por Francia, en virtud de la cláusula de asistencia mutua, de forma tal que se legitimó la intervención, en legitima defensa, frente a un "ataque" que, conceptualmente, dista de la definición estricta mantenida por las Naciones Unidas. En este sentido, la aportación de la cláusula parece más material que teórica. Es decir, a pesar de que el TUE no delimita qué ha de entenderse por un ataque armado que justifique la intervención prevista en su artículo 42.7, en la práctica ha suscitado una ampliación de dicho concepto en la lucha contra el terrorismo, auqnue los actos de terror perpetrados en territorio francés no sean atribuibles a un Estado. Si bien es ampliamente aceptado que un acto de terrorismo puede ser calificado como un acto de agresión internacional, si el mismo es atribuible a un Estado, en el caso en el que se activó la legítima defensa colectiva en la UE, a través de la cláusula de asistencia mutua, dista mucho de reunir ese imprescindible requisito de atribución. En consecuencia, consideramos que no es deseable que ningún sistema de legítima defensa, especialmente la colectiva, como la que se activó a través de la cláusula de asistencia mutua de la UE, no solo no debe quedar al margen de las exigencias contenidas en el artículo 51 de la Carta, sino que debe evitar que se convierta en un mecanismo *de facto* para ampliar el ámbito conceptual de los ataques armados que permitan una respuesta en legítima defensa. En consecuencia, la UE no debería seguir en esta línea, aportando conceptos autónomos de ataque armado para futuras y posibles activaciones de la cláusula de asistencia mutua, más aún, cuando al carecer de un

61 Resolución del Consejo de Seguridad de las Naciones Unidas 2249 (2015). La Resolución exhortó a adoptar "*todas las medidas necesarias, de conformidad con el derecho internacional, en particular la Carta de las Naciones Unidas y el derecho internacional de los derechos humanos, el derecho internacional de los refugiados y el derecho internacional humanitario, sobre el territorio que se encuentra bajo el control del EIIL, también conocido como Daesh, en Siria y el Iraq", redoblen y coordinen sus esfuerzos para prevenir y reprimir los actos terroristas cometidos específicamente por el EIIL, también conocido como Daesh, así como el Frente Al-Nusra, y todas las demás personas, grupos, empresas y entidades asociados con Al-Qaida y otros grupos terroristas designados por el Consejo de Seguridad de las Naciones Unidas, y los que acuerde el Grupo Internacional de Apoyo a Siria y corrobore el Consejo de Seguridad, de conformidad con la declaración del Grupo Internacional de Apoyo a Siria de 14 de noviembre, y erradiquen el cobijo que han establecido en partes importantes del Iraq y Siria*". Resolución 2249 (2015), aprobada por el Consejo de Seguridad en su 7565ª sesión, de 20 de noviembre de 2015. Doc. S/RES/2249 (2015).

procedimiento reglado para su activación la calificación jurídica de los actos de terrorismo se realizó unilateralmente por Francia[62].

Si, como vamos manifestando, hasta el momento, resulta necesario optar por un criterio restrictivo, a la hora de considerar los ciberataques como ataques armados, no sería deseable que se activase, en el futuro, la referida cláusula de asistencia mutua con una justificación en nuevos conceptos autónomos de ataque armado que resulten ilícitos o, al menos, de dudosa legalidad.

2.2. Estudio de los ciberataques en un conflicto armado no internacional.

Los ataques informáticos no pueden ser analizados exclusivamente como aquéllos que pueden originar un conflicto armado de carácter internacional. Antes bien, los mismos pueden originarse dentro del propio Estado, bien porque los agentes del Estado los originen contra su propia población, bien porque los agentes no estatales los dirijan contra el Estado. En cnsecuencia, es necesario plantearse la cuestión de si estos ciberataques pueden originar un conflicto armado no internacional. En la mayoría de las ocasiones, se tratará de supuestos en los que una situación de violencia colectiva, organizada o no, generará tensiones o disturbios internos en los que, eventualmente, las autoridades gubernamentales podrán invocar el estado de urgencia.

De este modo, en la tarea propuesta resulta también necesario tener en cuenta el artículo 1 del Protocolo Adicional II[63] a los Convenios de Ginebra de 1949 (en adelante, PAII) en el que se ofrece una definición más restringida, a la hora de delimitar qué es un conflicto armado no internacional. El PA II establece que, el mismo resulta de aplicación a los conflictos armados

> "que se desarrollen en el territorio de una Alta Parte Contratante entre sus fuerzas armadas y fuerzas armadas disidentes o grupos armados organizados que, bajo la dirección de un mando responsable, ejerzan sobre una parte de dicho territorio un control tal que les permita realizar

[62] GONZALEZ ALONSO, L.N., *¿Daños jurídicos colaterales? La invocación del artículo 42.7 del Tratado de la Unión Europea y la lucha contra el terrorismo internacional*, op. cit.

63 Protocolo II adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional, BOE de 7 de octubre de 1989.

operaciones militares sostenidas y concertadas y aplicar el presente Protocolo".

Es decir, el PA II incluye un requisito adicional, al exigir que las partes no gubernamentales ejerzan un control territorial "*que les permita realizar operaciones militares sostenidas y concertadas y aplicar el presente Protocolo*". Por otra parte, este PA II se aplica, únicamente, a los conflictos armados entre Fuerzas Armadas estatales y Fuerzas Armadas disidentes, u otros grupos armados organizados y no a los conflictos armados, que se libran sólo entre grupos armados no estatales.

En el presente contexto, es importante destacar que, las obligaciones relativas a la conducción de hostilidaes se aplican a ambas partes, en un conflicto armado interno. Sin embargo, a fin de que se aplique el PA II, la intensidad de los enfrentamientos debe ser mayor que lo que, tradicionalmente, se requiere para la aplicación del artículo 3 común a los Convenios de Ginebra. En consecuencia, conforme al artículo 1 (2) del PA II, no se prevé la aplicación del mismo a situaciones de tensiones internas, disturbios interiores y actos de violencia esporádicos. Además, el artículo 1 (1) del PA II exige que los grupos armados disidentes estén bajo la dirección de un mando responsable y que ejerzan, sobre una parte de dicho territorio, un control tal que les permita realizar operaciones militares y aplicar las garantías del Protocolo. Por lo general, se considera que esto constituye un umbral más alto para la aplicabilidad que lo dispuesto en el artículo 3 común[64]. Así, a juicio de CLAPHAM, hoy en día, incluso, en ausencia de un consenso acerca de una justificación teórica, no cabe duda de que los rebeldes están vinculados, como partes en el conflicto, no sólo por el artículo 3 común a los Convenios de Ginebra, sino también por las disposiciones del PA II[65]. Se trata pues, de considerar un tipo de situaciones, en las que el umbral de aplicabilidad del DIH no se ha alcanzado aún, pero en los que los derechos

64 CLAPHAM, A., *Obligaciones dimanantes de los derechos humanos para los actores no estatales en situaciones de conflicto.* International Review of the Red Cross. Septiembre de 2006, núm. 863 de la versión original; pp .2-37, en particular, p. 8.
65 CLAPHAM, A., *Obligaciones dimanantes*, op. cit; p.9.

humanos necesitan de la protección e intervención del CICR, motivada por la magnitud de las consecuencias humanitarias.[66]

En este aspecto, la doctrina ha multiplicado las iniciativas encaminadas a elaborar "*normas mínimas de humanidad*" para complementar los instrumentos convencionales[67]. En el Informe nacido de la XXVII Mesa Redonda sobre Problemas Actuales del Derecho Internacional Humanitario se concluyó con una propuesta que recoge la asunción de un criterio principal o necesario, combinado con otros, de carácter complementario. En consecuencia, para la acreditación de la existencia de un conflicto armado, se propuso como criterio necesario, el del uso de la fuerza armada por parte de un Estado. Entre los criterios de naturaleza complementaria, se citó la intención hostil (*animus belligerendi*), la duración en el tiempo de los actos de violencia y la intensidad de los mismos, en función de una acumulación de acontecimientos, siempre teniendo en cuenta que la calificación de conflicto armado no internacional implica un mínimo de organización, por parte de cada beligerante. En consecuencia, se exigirá que los grupos o fuerzas armados disidentes estén dirigidos por un mando responsable y que esta estructura jerárquica disponga de un grado de efectividad suficiente para poder cumplir las obligaciones que le incumben, en virtud del DIH. Esta última exigencia dimana, implícitamente, de la referencia a la noción de "*partes en el conflicto*", que figura en el artículo 3. Sin embargo, parece delicado atribuir ese calificativo a un grupo que no disponga de una estructura jerárquica, al menos, básica.

Si atendemos a estos requisitos está claro que los ciberataques, hasta ahora más virulentos, adolecen de alguno de ellos, por lo que resulta comprensible la

66 Así se expresa MINNIG, Jefe de la Delegación del CICR en Buenos Aires, en junio de 2008, MINNIG, M., *La protección de las personas en situaciones de violencia interna.* Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/america-internal-violence-itw-070708.htm. Fecha de consulta, junio 2013.

67 En este sentido se expresa el informe resultante de la XXVII Mesa Redonda sobre Problemas Actuales del derecho internacional humanitario. CICR, *El derecho internacional humanitario y los retos de los conflictos armados contemporáneos.* Informe resumido preparado por el Comité Internacional de la Cruz Roja resultante de la XXVII Mesa Redonda sobre problemas actuales del DIH: Derecho Internacional Humanitario y otros regímenes jurídicos. Interacción en las situaciones de violencia. Instituto Internacional de Derecho Humanitario, San Remo, Italia. Noviembre de 2003; p.5.

inicial reserva a la aplicación del DIH. Si bien es cierto que los ataques sufridos por Estonia o Lituania fueron de la entidad suficiente para, al menos, plantear algún tipo de respuesta por parte de la Comunidad Internacional, basada en la aplicación del DIH, no es menos verdad que sus características, difícilmente, permitían su encuadramiento en la definición de conflicto armado no internacional citada. Conforme al primero de los requisitos, es comprensible la duda inicial, a la hora de definir estos ciberataques como manifestaciones de una fuerza armada. Pero, además, atendiendo al resto de los elementos, llamados complementarios, resulta imposible detectar esa mínima organización requerida y, aun menos, la existencia de un mando responsable y una estructura jerárquica efectiva. De esta forma, a pesar de su prolongación en el tiempo y la intensidad de los mismos, a duras penas podría haberse calificado ninguna de las dos situaciones como conflicto armado no internacional.

Por otra parte, reulta que la duración de los actos de violencia puede desempeñar un papel importante, en la distinción entre un conflicto armado no internacional y una situación de tensión interior o disturbios internos[68]. Sin embargo, este criterio no parece tener una relevancia suficiente para ser tenido en cuenta de modo autónomo, sino, a lo sumo, de forma complementaria, junto con otros que pueden resultar más determinantes y que, en cualquier caso, han de concurrir.

Igualmente, atendiendo al criterio de las fuerzas o tácticas utilizadas[69], la situación puede calificarse como conflicto armado no internacional, únicamente, si el nivel de violencia impide a las autoridades competentes, en materia de mantenimiento del orden, controlar una situación, de forma que las circunstancias constatadas requieran la intervención de las Fuerzas Armadas.

Pues bien, este criterio resulta, de todo punto inservible, a la hora de determinar la aplicación de las normas del DIH, en los casos de los ciberataques de los que se tiene conocimiento. Antes bien, la previa calificación será la que, en

68 Así se puso de manifiesto, igualmente, en el aludido informe resultante de la XXVII Mesa Redonda. CICR, *El derecho internacional humanitario y los retos de los conflictos armados contemporáneos*, doc. cit.; p.6.
69 *Ibidem*; p.6.

todo caso, determine si nos encontramos ante una situación que afecte a la seguridad interna del Estado en cuestión o, por el contrario, a la Defensa Nacional, de modo que no puede considerarse, en sí mismo, un criterio válido para la calificación necesaria.

Por último, el documento que se examina aboga por una cuarta serie de criterios, configurados en función de la intensidad de los actos de violencia. En este grupo se engloban los precedentes propuestos, a la vez que se permite la aceptación de factores complementarios, tales como el número de personas implicadas en los actos de violencia o de víctimas. No parece, sin embargo, que un aspecto meramente cuantitativo pueda resultar determinante, a la hora de proceder a una calificación eminentemente jurídica, como la que se pretende. No puede obviarse, por otra parte, la dificultad intrínseca de la determinación de ese elemento numérico[70].

La oportunidad y prudencia en la elección de los criterios que se analicen en orden a calificar un ciberataque como ataque armado resultan de suma importancia, pues no es descartable, como a lo largo del presente trabajo se expondrá, que un ataque de dicha índole pueda desencadenar una ciberguerra o, en su caso, un conflicto bélico de otra naturaleza. Como posteriormente se analizará con mayor detalle, estos ataques podrán suponer, bien el desencadenamiento de las hostilidades, bien la respuesta que el Estado ofrezca como consecuencia de un ataque previo, sea este convencional o virtual.

Nada impide, asimismo, que dichos ataques o respuestas se den en el ámbito interno del Estado y que el mismo los lanzara contra personas o entidades de carácter civil, como ocurrió en el caso de Bielorrusia.

Tanto en la relación con los conflictos armados internacionales como no internacionales podemos concluir que se hace preciso abogar por los criterios que, sin abandonar las fuentes del Derecho Internacional, proponen una interpretación restrictiva. Si ante la recepción de un ciberataque se adoptara una visión excesivamente amplia, podría originar la consideración de ataque armado respecto de actividades en la red que, posteriormente, podrían revelarse

70 *Ibidem*; p. 7.

inofensivas o, a lo sumo, meramente delictivas, sin alcanzar la entidad que se exige respecto de un ataque armado. Esta situación, habida cuenta la frecuencia con que se producen estos ciberataques, así como la aparición de los mismos, en contextos en los que la tensión política es evidente, podría originar respuestas desproporcionadas y dar lugar, por ende, a un agravamiento de la situación. Se impone, por lo tanto, la adopción de un criterio restrictivo que, en todo caso, proporcione una respuesta a supuestos concretos que ya se han producido y a otros que, en el futuro, pudieran producirse en un contexto similar.

En consecuencia, el criterio defendido por los autores del Manual de Tallin, cuando pretende aplicarse ya no en un plano meramente teórico, sino teniendo presentes los supuestos concretos de los que se tiene constancia, permite la conceptualización de ciertos ciberataques, como Stuxnet, como ataques armados, con las consecuencias que, desde el punto de vista jurídico, ello origina, a la luz de la legalidad examinada.

Sin embargo, la calificación jurídica de los ataques únicamente supone un punto de partida, de manera que la exigencia de responsabilidad del Estado, en supuestos como los que aquí se traen a colación, aún se enfrenta a varios retos. En primer lugar, porque, incluso considerado el ciberataque como ataque armado, posteriormente habrá que determinar si el mismo proviene de un agente del estado o de un individuo que actúe como agente no estatal. En el caso de que se constaten durante un conflicto armado, será preciso dirimir si la operación informática, en cuestión, es atribuible a un miembro de las Fuerzas Armadas de un Estado parte en el conflicto o no y probar, si dicho componente de las Fuerzas Armadas actuaba cumpliendo una orden y no a título particular. Como se verá en el momento de atender a las cuestiones relacionadas con la atribución del hecho ilícito, la responsabilidad del Estado podrá originarse, asimismo, cuando el Estado agresor o "atacante" asuma esa actividad como propia[71].

71 En relación con la responsabilidad derivada de la actuacion de los miembros de las Fuerzas Armadas, vease, RENAUT, C., *The impact of military disciplinary sanctions on compliance with international humanitarian law.* International Review of the Red Cross, vol. 90, no. 870 June 2008; pp. 319-326.

En cualquier caso, es evidente que la amenaza virtual puede llegar a ser un riesgo real y, en consecuencia, originar una situación en la que sea precisa la actuación de los medios puestos a disposición de la Defensa Nacional.

2.3. El tratamiento de los ciberataques armados en el Código Penal Militar español.

La atención al concepto de ataque armado ofrecido por las Organizaciones Internacionales, tanto en el ámbito universal y como en el regional europeo, que han sido objeto de análisis, se justifica por la pertenencia de España a las mismas y nuestra involucración en futuras misiones que éstas lideren. Es momento ahora de descender al ámbito nacional y abordar la conceptuación que se realiza de los ataques informáticos como ataques armados, en el ordenamiento jurídico español.

En este sentido, el Derecho español ha dado un paso importante en la delimitación conceptual que se aborda. Así, en la última reforma del Código Penal Militar (en adelante, CPM) ya se incorporan, al catálogo de definiciones, dos novedades que han de verse como un claro avance en la conceptuación de los ciberataques, que queda reflejado en la definición del servicio de armas. El artículo 6 del CPM en su párrafo segundo, establece que:

> "A los efectos de este Código, son actos de servicio de armas todos los que requieren para su ejecución el uso, manejo o empleo de armas, cualquiera que sea su naturaleza, conforme a las disposiciones generales aplicables o a las órdenes particulares debidamente cursadas al respecto, así como los actos preparatorios de los mismos, ya sean individuales o colectivos, desde su iniciación con el llamamiento a prestarlo hasta su total terminación, y cuantos actos anteriores o posteriores al propio servicio de armas se relacionen con éste o afecten a su ejecución. Asimismo, tendrán esta consideración los actos relacionados de forma directa con la navegación de buques de guerra o de la Guardia Civil, o el vuelo de aeronaves militares. También la tendrán los servicios de transmisiones, comunicaciones o informáticos, detección y análisis del espacio radioeléctrico o cibernético, imágenes o datos y cualesquiera otros servicios de vigilancia y control de los espacios en que se desarrollen las operaciones militares".

La equiparación de la prestación del servicio de transmisiones, comunicaciones o informáticos, de detección y análisis del espacio radioeléctrico y cibernético al servicio de armas supone una novedad, acorde con los tiempos y, además, un gran avance en la delimitación conceptual que se evidencia tan necesaria.[72] Ello quiere decir que, en el ámbito penal militar español, no se ofrece ninguna diferencia al hecho de prestar un servicio con un arma convencional o cibernética. La alusión, en concreto, a la *naturaleza* del arma, aporta una dimensión realmente amplia a la conceptuación de los ciberataques A partir de esta previsión, puede afirmarse que el método de combate que se elija, en el uso del arma en concreto, quedará amparado por dicha definición. Por lo tanto, la responsabilidad que se exija al militar, a quien corresponda cualquiera de esos servicios, será la misma, con independencia del arma que en la prestación del mismo haya portado o usado. En consecuencia, los actos cometidos en el desempeño de este servicio han de tener idéntica consideración, desde un puno de vista conceptual, ya se trate, pues, del empleo de armas convencioanles o virtuales. Así, cuando el artículo 67 castiga al militar que abandone un servicio de armas, hay que entender incluido, en el tipo penal, a quien preste un servicio informático, sin que pueda este militar acogerse al tipo descrito en el segundo párrafo, relativo al abandono de otros servicios, cuya comisión se castiga con una pena de menor gravedad[73].

72 Codigo Penal Militar, aprobado por Ley Orgánica 14/2015, de 14 de octubre. BOE núm. 247, de 15 de octubre de 2015.

73 El artículo 67 del Código Penal Militar, establece que *"1. El militar que abandonare un servicio de armas será castigado:*

1. º Con la pena de diez a veinte años de prisión, cuando tuviere lugar frente al enemigo, rebeldes o sediciosos.

2.º Con la pena de cinco a quince años de prisión, cuando tuviere lugar en situación de conflicto armado o estado de sitio, fuera de las situaciones expresadas en el apartado anterior, o en circunstancias críticas.

3. º En los demás casos, con la pena de tres meses y un día a dos años de prisión.

2. El abandono de cualquier otro servicio, cuando tuviere lugar en situación de conflicto armado o estado de sitio, frente al enemigo, rebeldes o sediciosos o en circunstancias críticas, será castigado con la pena de seis meses a seis años de prisión.

3. El militar que no se presentare al cumplimiento de los servicios mencionados en los números anteriores, o incumpliere sus obligaciones ocasionando grave daño al servicio, será castigado con las penas allí previstas en su mitad inferior".

De igual modo favorable hay que recibir la novedad, en relación al tratamiento de la figura del centinela[74], es decir, el que "*en acto de servicio de armas y cumpliendo una consigna, guarda un puesto confiado a su responsabilidad, portando a la vista el arma de fuego que por su cometido le corresponda*". Esta previsión no es sino una lógica consecuencia de la anterior. En efecto, una vez el servicio informático es considerado un servicio de armas, a quien se halla en el desarrollo del mismo ha de otorgársele idéntica protección que al centinela que defiende una posición física. En consecuencia, cuando el artículo 34 del CPM castiga a quien desobedezca o se resista al cumplimiento de las órdenes del centinela, hay que entender incluido a quien presta servicio, como operador de una red informática. En otros supuestos, como el recogido en el artículo 45, la orden relativa a la prestación de un servicio de armas, constituye una conducta agravada respecto del tipo básico[75].

Por último, cabe hacer una breve referencia al concepto que, de ciberataque, se recoge en la Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (en adelante, MCCD) que lo define como la "*Acción producida en el ciberespacio que*

---

74 El artículo 4, literalmente, establece: "*1. Es centinela, a los efectos de este Código, el militar que, en acto de servicio de armas y cumpliendo una consigna, guarda un puesto confiado a su responsabilidad, portando a la vista el arma de fuego que por su cometido le corresponda. 2. Tienen además dicha consideración los militares que sean:*

a) Componentes de las guardias de seguridad en el ejercicio de su cometido;

b) Operadores de las redes militares de transmisiones, comunicaciones o informáticas durante el desempeño de sus cometidos; y

c) Operadores de sistemas electrónicos de vigilancia y control de los espacios confiados a los Centros o estaciones en que sirven u observadores visuales de los mismos espacios, durante el desempeño de sus cometidos".

Asimismo, tendrán esta consideración los actos relacionados de forma directa con la navegación de buques de guerra o de la Guardia Civil, o el vuelo de aeronaves militares. También la tendrán los servicios de transmisiones, comunicaciones o informáticos, detección y análisis del espacio radioeléctrico o cibernético, imágenes o datos y cualesquiera otros servicios de vigilancia y control de los espacios en que se desarrollen las operaciones militares". Código Penal Militar, doc.cit.

75 El artículo 44 aquí citado, determina que "*1. El militar que se negare a obedecer o no cumpliere las órdenes legítimas de sus superiores relativas al servicio será castigado con la pena de tres meses y un día a dos años de prisión. 2. Si se tratare de órdenes relativas al servicio de armas, se impondrá la pena de seis meses a seis años de prisión*". *En el mismo sentido arriba expresado, puede entenderse la previsión del artículo 70 del mismo Texto Legal, cuando establece: "El militar que, en acto de servicio de armas, voluntaria o imprudentemente se embriagare o consumiere drogas tóxicas, estupefacientes o sustancias psicotrópicas, de modo que su capacidad para prestarlo desaparezca o disminuya, será castigado con la pena de tres meses y un día a un año de prisión. Cuando se cometa el hecho por un militar que, en cualquier acto de servicio, ejerciera el mando, se impondrá la pena de prisión de seis meses a dos años*".

compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan[76]". Desde un punto de vista jurídico, parece evidente que a la acción que el artículo describe le serán de aplicación las consideraciones que han sido expuestas, en relación al ataque armado. Ciertamente, el contenido eminentemente técnico de la disposición, así como su rango normativo parecen aconsejar que la definición de ciberataque se acomode a dichas notas características y que, de ese modo, prevalezca el concepto jurídico de ataque que se ha expuesto.

3. LA OBLIGACIÓN INTERNACIONAL VINCULANTE PARA EL ESTADO. DELIMITACIÓN DEL ACERVO JURÍDICO APLICABLE A LOS CIBERATAQUES.

A la vista de lo expuesto hasta ahora, puede concluirse que este novedoso elemento cibernético podrá ser utilizado en un conflicto armado internacional o que no revista ese carácter. En el desarrollo del mismo, las Fuerzas Armadas de los Estados beligerantes podrán utilizar los ataques informáticos como un método de combate. En el desarrollo de este combate, e incluso con carácter previo, los ciberataques podrán alcanzar la entidad de ataque armado, aun cuando los mismos se califiquen en función de las tesis restrictivas, antes expuestas. Asimismo, parece probable que los Estados, cada vez con mayor frecuencia, hagan uso de este método de combate. En consecuencia, toda vez que no existe una previsión específica en el Derecho Internacional que determine la licitud o ilicitud del lanzamiento de los ciberataques, es necesario proponer el acervo normativo que, en su caso, ha de resultar de aplicación.

De este modo, podrá asimismo abordarse la cuestión de si ese ataque armado puede constituir un hecho ilícito por transgredir una norma de carácter internacional, vinculante para el Estado que origina o no impide un ciberataque.

76La Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa
de las Fuerzas Armadas fue publicada en el Boletín Oficial de Defensa núm. 40, de 26 de febrero de 2013.

En esta labor es preciso, en primer lugar, discernir cuál será la norma de Derecho Internacional cuya violación conllevará la exigencia de responsabilidad internacional. Si nos atenemos al concepto admitido por la Comisión de Derecho Internacional (en adelante, CDI) [77] el hecho ilícito se debe a la violación de una obligación internacional, cuando un acto del Estado no resulte conforme a la exigencia derivada de esa obligación internacional.

Resulta necesario, por lo tanto, determinar si un ciberataque podrá ser contrario a una norma de Derecho Internacional y, en consecuencia, delimitar cuál será la obligación internacional violada, contenida en la normativa de DIH. Esta cuestión surge, en primer lugar, de la evidencia de que ningún Tratado Internacional ha recogido el empleo de internet, como un arma de guerra. Por otra parte, su existencia, aunque extendida, resulta lo suficientemente reciente como para contar con una practica internacional ni una mínima opinio iuris que permita la aplicación de una costumbre internacional.

En este contexto habrá que analizar pues, la legalidad internacional, a la que se halla vinculado el Estado, en el desarrollo del conflicto para ver si el uso de un ciberataque puede o no, producir la violación de una obligación internacional.

3.1 El tratamiento jurídico de internet a la vista de su condición de arma de doble uso.

Del análisis conceptual de los ciberataques, se ha concluido que internet puede ser calificado jurídicamente como un ataque armado y, en consecuencia, ser utilizado como método de combate. Sin embargo, hay que tener en cuenta que la red no constituye, únicamente, un método con el que atacar o defenderse, en función de los distintos tipos de operaciones cibernéticas en el conflicto armado. Al contrario, la posibilidad de utilizar la red con fines inofensivos e, incluso beneficiosos, para el individuo y la sociedad, de hecho, es realizada con mayor frecuencia que su uso como método de combarte.

77 Las distintas acepciones se recogen en el comentario 2) al artículo 12 del Proyecto de artículos.

En primera instancia, resulta determinante establecer cuándo la utilización de internet constituye un hecho ilícito, de conformidad con el DIH y, por lo tanto, derivarse la exigencia responsabilidad internacional del Estado que lo cometa.

Esta cuestión exige un nuevo análisis conceptual, como consecuencia del que se ha realizado en relación a la naturaleza jurídica de los ciberataques, pues es preciso concretar, en primer lugar, qué tipo de armas estamos examinando para, posteriormente, deslindar el régimen jurídico que les sea aplicable.

La posibilidad de ese uso dual de la red se evidencia determinante e impone el análisis de internet, desde una perspectiva que tenga en cuenta que el elemento cibernético es susceptible de un uso lícito como ilícito. En consecuencia, parece evidente que el análisis de la legalidad internacional que sea aplicable a los ciberataques se examine en analogía con la legalidad que se aplica a otras armas que también permiten un uso inofensivo e incluso beneficioso. Por lo tanto, se requiere atender al estudio del régimen jurídico que ha sido establecido para las armas de doble uso.

Son varias las armas que, desde hace décadas, comparten esta naturaleza dual y la asimilación de las mismas a internet se justifica por varios motivos. En primer lugar, hay que mencionar que la red ofrece posibilidades de uso militar. Incluso, su origen se encuentra en el ámbito militar, de la misma forma que ya ocurrió con la energía nuclear, el radar o el láser[78]. Además, en analogía con estos elementos citados, el aprovechamiento en el ámbito civil, resulta incuestionable.

En este sentido, puede distinguirse entre los llamados «productos de doble uso», que son definidos como aquellos que han sido desarrollados para una serie de aplicaciones comerciales concretas y que, además, pueden ser utilizados, directamente o con modificaciones menores, en aplicaciones militares y, por otra parte, las «tecnologías de doble uso» que son las que permiten obtener este tipo

78 Estas cuestiones, aunque de forma elemental, son explicadas en el documento INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATEGICOS. Inventos del mundo militar que nos cambiaron la vida. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/espacio_docente/Inventos_MundoMilitar_CambioVida.pdf. Fecha de consulta, enero de 2017.

de productos[79]. En la actualidad, la tendencia contraria también ha sido constatada, de modo que determinadas tecnologías de origen y uso civil, son objeto de un claro aprovechamiento en el ámbito militar.[80].

La consecuencia que, desde una perspectiva jurídica, implica esta naturaleza dual se concreta, desde hace décadas, en la necesidad de prohibir o de limitar la utilización de estas armas, en aras al aseguramiento de la paz y seguridad mundiales. Esta calificación resultará de utilidad, pues, a la hora de entender el modo en que internet ha de ser utilizado, en el desarrollo del combate. En consecuencia, el examen del precedente orientará la actividad futura, en relación a un método que actualmente carece de regulación expresa y del que, hasta la fecha, no ha originado la suficiente práctica, por parte de los Estados. Ello, además, llevará a que se perfilen las condiciones que permitan un uso lícito y seguro de dicha red.

El desafío que ha supuesto la aparición de armas, no contempladas por el DIH convencional, o la utilización de elementos, hasta ahora inofensivos, con fines bélicos ha originado respuestas jurídicas de diversa naturaleza. En unos casos, se ha optado por la elaboración de Tratados internacionales específicos, que han venido a cubrir la laguna que el Derecho Internacional presentaba en ese concreto ámbito. En otros supuestos, la respuesta ha venido de la mano de la aplicación de la analogía, al atender el llamado "*imperativo de humanidad*"[81].

---

79 Esta definición es la aportada por QUINTEIRO BLANCO, M., *Consideraciones generales sobre las tecnologías de doble uso*. Tecnologías de doble uso en la industria de la Defensa. Cuadernos de Estrategia núm. 67. Centro Superior de Estudios de la Defensa Nacional; pp. 59 a 105, en particular, p. 97.

80 Los ejemplos en este sentido son ofrecidos por RIOLA RODRIGUEZ, que expone, entre ellos el procesamiento masivo, conocido como *Big data*, «*de un gran auge hoy día, donde los sistemas de procesamiento, ordenadores, están intercomunicados en internet de forma natural, y su agrupamiento de forma distribuida o en grandes centros de computación permiten aplicar su gran potencia de cálculo a problemas complejos. Su aplicación en el mundo civil nace a la sombra de las grandes redes sociales, donde el interés económico se centra en obtener información sobre los clientes para identificar determinados usuarios para determinados productos. Su aplicación en el mundo militar pasa por labores de vigilancia de las redes para prevención de ataques terroristas o adquisición de información de inteligencia*». RIOLA RODRÍGUEZ, J.M. *La situación actual de las tecnologías de doble uso*. Desarme y control de armamento en el siglo XXI: limitaciones al comercio y a las transferencias de tecnología. Cuadernos de Estrategia núm. 169. Instituto Español de Estudios Estratégicos. Centro Superior de Estudios de la Defensa Nacional. Diciembre 2014; pp. 157 a 191, en particular, p. 174.

81 Así se desprende de la Nota presentada por Jakob Kellenberger, Presidente del Comité Internacional de Cruz Roja, tras la 34ªMesa Redonda. CICR, *International Humanitarian Law and New Weapon Technologies*. Statement 34th Round Table on Current Issues of International

En un principio, la elaboración de un Tratado Internacional, que permitiera regular el uso de los ciberataques, podría contemplarse como la solución definitiva a la indefinición conceptual que sufre esta materia. De este modo, partiendo de una definición consensuada, podría darse una respuesta, comúnmente aceptada por los Estados, que permitiera despejar, definitivamente, la incógnita sobre los supuestos en los que el Estado incurriría en ilicitud al lanzar un ciberataque. La frecuencia de este tipo de ataques, sufridos no sólo por los individuos, sino también por los Estados, como ocurrió en el caso de Georgia o en el lanzamiento del virus Stuxnet, avalaría tal propuesta, pues es evidente que ese peligro puede ser percibido de forma cercana [82]. Más aún, podría sostenerse esta propuesta cuando el lanzamiento de este virus ha sido considerado un potencial peligro para la paz y seguridad mundiales. En este sentido, pues, algunos autores lo han llegado a considerar el punto de partida en una escalada en el armamento cibernético, que se ve facilitada y acelerada, además, por la intrínseca naturaleza de internet, que permite compartir y adquirir conocimientos por la red, de forma sencilla e inmediata. [83]

Las anteriores circunstancias podrían provocar, en un futuro, una proliferación de las armas cibernéticas, similar a la que en su día ocurrió en

---

Humanitarian Law, San Remo, 8-10 September 2011. Keynote address by Dr. Jakob Kellenberger, President, ICRC. Documento disponible en el sitio web: https://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm. Fecha de consulta, mayo 2013.

82 La experimentación de los efectos negativos de las armas químicas resultó determinante para la prohibición de su uso tal y como hoy es conocida. Así lo explica MATAMOROS MARTINEZ, al poner de manifiesto la evolución histórica de esta materia: "*La primera norma internacional que prohibió el empleo de venenos y armas venenosas fue el Reglamento del II Convenio de La Haya, sobre la Guerra Terrestre, de 1899 (art. 23). La misma regla apareció reproducida por el Reglamento del IV Convenio de La Haya, de 1907 (art. 23). Por otro lado, a través de la Declaración IV.2 de La Haya, de 1899, los Estados parte acordaron abstenerse de emplear en la guerra proyectiles cuyo único efecto fuera la difusión de gases asfixiantes o deletéreos. La negativa experiencia del empleo a gran escala de armas químicas durante la I Guerra Mundial tuvo un inmediato reflejo en el ámbito normativo*". MATAMOROS MARTÍNEZ, R., *El marco jurídico del bioterrorismo*. Anuario Jurídico y Económico Escurialense, XXXVII (2004); pp. 17 a 46, en particular, p. 21.

83 Así lo han puesto de manifiesto SINGER y FRIEDMAN, quienes, por ese motivo, han calificado el virus Stuxnet como "*una victoria pírrica*". Estos autores entienden que, si bien la introducción de dicho virus, destruyó las capacidades de Irán para seguir generando una amenaza nuclear, del mismo modo, supuso el comienzo de una escalada en la generación de armamento cibernético, de manera que, consideran la ventaja inicialmente conseguida, pronto se manifestó en un riesgo potencial. SINGER, P. W. and FRIEDMAN, A. *Cybersecurity and cyberwar. What everyone needs to know*. Oxford University Press. Oxford 2014; p.156.

relación a las armas químicas y que ha supuesto la transformación de las mismas. Las armas químicas han pasado de ser unas armas específicas y con un uso limitado al contexto bélico, a tener un carácter difuso cuyo objetivo es, en ocasiones, el ámbito civil. En este ámbito civil, la amenaza más peligrosa ya no proviene exclusivamente de actores estatales, sino que también tiene su origen en actores no estatales. Esa misma característica, determinante de la actual naturaleza de dichas armas, puede predicarse de internet. De forma evidente, la red no ha tenido un uso bélico desde el principio, pero sí que puede decirse que cuando se utiliza maliciosamente, la amenaza puede provenir, igualmente, de actores no estatales y, en diversas ocasiones, se ha puesto de manifiesto que su objetivo ha sido civil[84].

En el caso de las armas químicas, su proliferación ha pretendido ser mitigada a través de la implantación de un mecanismo de verificación y de un régimen de inspecciones, ambos contenidos en el Tratado Internacional que las regula[85]. La Convención para la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de las Armas Químicas y sobre su Destrucción Convención (en adelante, CAQ) establece la norma global contra el uso y el desarrollo, la producción y el almacenamiento de armas químicas, constituyendo, así, la base legal contra la proliferación de las mismas. La CAQ impone, asimismo, un régimen de inspecciones, que se basa en una serie de declaraciones iniciales y anuales, formuladas por los Estados Parte, en relación a las armas químicas que poseen y la industria afín[86]. Asimismo, la CAQ prevé un sistema de desarme, por el que los Estados poseedores de armas químicas deben de destruir sus existencias por completo antes del 2012[87].

---

84 Así ocurrió en los ciberataques que aquí se vienen citando, ocurridos en Estonia, Lituania y Bielorrusia, principalmente.

85 Este Tratado Internacional es la Convención para la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de las Armas Químicas y sobre su Destrucción. París, 13 de enero de 1993.

86 Así puede comprobarse en los artículos IV y ss. de la Convención para la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de las Armas Químicas y sobre su Destrucción.

87 Al respecto, puede consultarse a BORREDA JUSTE, que explica este régimen de control de las armas químicas y biológicas y, además, aclara que los Estados poseedores son Estados Unidos, la Federación Rusa, India, Libia, Albania y un Estado-Parte. Por "un Estado-Parte", ha de

Sin embargo, este mecanismo, puesto en funcionamiento para el control de este tipo de armas, no parece que pudiera resultar igualmente efectivo, en el caso de que se pretendiera un control similar de las armas cibernéticas. La completa asimiliacion del régimen jurídico no parece viable si tenemos en cuenta la virtualidad de este nuevo método de combate y su fácil ocultación, que dejaría en manos de la buena voluntad de los Estados, la eficacia del control. En idéntico sentido procede manifestarse en relación al sistema implantado por la Convención relativa a las armas bacteriológicas (en adelante, CAB)[88]. En la CAB, sólo las Medidas de Fomento de la Confianza, consistentes en el intercambio de datos e información y en declaraciones de actividades pasadas o presentes de relevancia para la convención, permiten el control de estas armas.[89] A ello hay que añadir que, al igual que sucede con estas armas de doble uso, también en el caso de internet será muy difícil delimitar si el futuro uso que se dé al desarrollo tecnológico correspondiente, va a resultar lícito o no[90].

Asimismo, la imposiblidad de adaptar cualquiera de estos sistemas como referencia para la regulación de internet, encuentra el obstáculo de que, el control de seguridad que ha de observarse, en el proceso de elaboración, no resultará sencillo, a diferencia de lo que puede ocurrir en otras armas de doble uso.

En el caso de la proliferación nuclear ocurre otro tanto, en relación al ciclo del combustible nuclear, pues resulta extremadamente complicado discernir si una planta de enriquecimiento de uranio se encuentra trabajando en un objetivo lícito, como puede ser la producción de energía, o ilícito, como la producción de

---

entenderse el Estado de Corea del Sur que, como expresa el autor, puso de manifiesto sus reticencias a la referencia expresa de su pertenencia a la Convención. BORREDA JUSTE, F. en, *Las armas químicas y biológicas. Respuestas al reto de la proliferación*. Documentos de Seguridad y Defensa, núm. 27. Centro Superior de Estudios de la Defensa Nacional; pp. 73 a 85, en particular, p. 76.

88 Convención para la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de las Armas Biológicas (Bacteriológicas) y Tóxicas y de su Destrucción de 10 de abril de 1972.

89 BORREDA JUSTE, F., *Las armas químicas y biológicas*, op.cit.; p. 79.

90 Esta misma dificultad ha sido puesta de manifiesto en relación a otras armas consideradas de doble uso, con anterioridad al desarrollo de internet. En ese sentido se expresa CÁNOVAS SÁNCHEZ, al afirmar que, «*Por ello inicialmente, es muy difícil diferenciar cuando un producto químico tóxico es fabricado con fines industriales, farmacéuticos, alimenticios, etc. o con fines totalmente opuestos, es decir también con fines malignos. Este punto crea una gran complejidad y por ello es necesario unos estrictos controles de seguridad para garantizar la limpieza de los procesos*». CÁNOVAS SÁNCHEZ, B. *Capacidades militares en temas NBQ-R*. Las armas NBQ-R como armas de terror. Monografías del CESDEN núm. 120. Centro Superior de Estudios de la Defensa Nacional. Mayo 2011, pp. 141 a 197, en particular, p. 158.

armas nucleares. Como paradigma del arma de doble uso, nos encontramos con el hecho de que el uranio altamente enriquecido, presente en la producción de estas armas, también es utilizado para otros fines lícitos, como la propulsión de buques o la investigación en ciertos tipos de reactores. Esta circunstancia obliga, consecuentemente, a un control internacional de estos materiales[91].

Esa escalada en la adquisición y uso que se prevé pueda ocurrir en relación al armamento cibernético, antes mencionada, no dista de la que se ha producido con otras armas de doble uso. Ello ha originado la creación de regímenes de no proliferación y desarme, tendentes a mitigar el problema de la dispersión y el aumento de armamento, que podría "causar serios desequilibrios y tensiones con consecuencias catastróficas" [92]. En el ámbito de las armas nucleares, el sistema multilateral de no proliferación gira en torno al Tratado de No Proliferación (en adelante, TNP)[93] que, a pesar de las críticas que ha recibido, ha sido capaz de contener una proliferación de armas nucleares que hace 35 años se temía aún más acelerada que ahora[94].

El citado TNP contiene una serie de obligaciones jurídicas, vinculantes para los denominados por el propio Tratado, Estados nucleares. Estos, llamados Estados nucleares, se comprometen a no traspasar armas nucleares u otros dispositivos de esta clase. Además, tres de los Estados nucleares, en concreto, Estados Unidos, Reino Unido y la Unión de Repúblicas Socialistas Soviéticas (URSS), una vez aprobado el Tratado, se comprometieron mediante declaraciones formales a actuar a través del Consejo de Seguridad de Naciones Unidas y de este modo, tomar las medidas necesarias para contrarrestar cualquier agresión con armas nucleares o amenaza contra un Estado no nuclear[95]. También, para los Estados llamados no nucleares, se establecen obligaciones pues éstos, se

91 Así lo pone de manifiesto QUEVEDO RUIZ, J.R., en *Naciones Unidas y la lucha contra la proliferación de las armas de destrucción masiva. Logros y expectativas*. Naciones Unidas como principal elemento del multilateralismo del siglo XXI. Monografías del CESDEN núm. 109. Centro Superior de Estudios de la Defensa Nacional. Febrero 2009; pp. 129-178, en particular, p. 148.

92BORREDA JUSTE, F. *Las armas químicas y biológicas*.op. cit; p.73.

93 Tratado sobre la No Proliferación de las armas nucleares, firmado en Londres, Moscú y Washington el 1 de julio de 1968.

94 QUEVEDO RUIZ, J.R., *Naciones Unidas y la lucha contra la proliferación de las armas*, op.cit.; p. 144.

95 *Ibidem*; p. 144.

comprometen a no fabricar armas de este tipo u otros artefactos nucleares. Por último, las obligaciones mutuas descritas en el TNP se acompañaron de un sistema de verificación o de salvaguardias internacionales y unas garantías relativas al derecho a utilizar la tecnología nuclear para usos pacíficos[96] .

Las razones que pudieran impulsar a los Estados, al cumplimiento de las obligaciones, recogidas en los acuerdos multilaterales relativos a las Armas de Destrucción Masiva, podrían ser su interés en proteger su imagen hacia la Comunidad Internacional, ante la que pretenda presentarse ofreciendo cierta fiabilidad. Asimismo, puede deberse al interés en procurarse el acceso a la tecnología, la asistencia técnica y materiales para su empleo en usos pacíficos. Por último, no puede dejar de tenerse en cuenta que el temor a posibles sanciones resulta un acicate en el cumplimiento de las obligaciones impuestas.

Sin embargo, de tales motivaciones no puede inferirse una completa adhesión a este régimen por parte de los Estados, pues también han sido puestas de manifiesto aquéllas motivaciones que, por el contrario, inclinan a los mismos a mantenerse al margen de estos acuerdos multilaterales o incumplir las obligaciones que contienen. Entre estas últimas, QUEVEDO RUIZ destaca el miedo que puede suscitar en un Estado, el hecho de que un adversario real o potencial desarrolle o haya desarrollado capacidades en este ámbito. También se menciona, entre ellas, el aseguramiento de una respuesta que resulte contundente respecto a la superioridad militar de un adversario, sea éste real o potencial, sobre todo en regiones inestables. Asimismo, se destaca el interés por aumentar la influencia estratégica regional o el interés por aumentar el prestigio interno de un régimen de gobierno no democrático, como forma de perpetuarse en el poder. Todo ello, a juicio del mismo autor, además, resulta favorecido por el bajo coste que supone la adquisición de las llamadas capacidades asimétricas[97].

Pudiera pensarse que, a falta de una expresa regulación jurídica de las armas cibernéticas, el ejemplo ofrecido por Tratados Internacionales en los que, detalladamente, se regula el uso de otras armas con las que aquéllas comparten

96 *Ibidem*; p. 145.
97 *Ibidem*; pp. 161 y 162.

características esenciales, pudiera ser tomado como un primer paso en esa futura regulación. No cabe duda de que la implantación de medidas, como las que han sido apuntadas, tales como los sistemas de verificación, el compromiso de los Estados en el intercambio de datos e información y en la formulación de declaraciones de actividades, la existencia, incluso de una norma global contra el uso de un determinado armamento, el desarrollo de un régimen de desarme o el compromiso, plasmado en un Tratado Internacional, de que la actuación de los Estados, en una determinada materia, se rija a través del Consejo de Seguridad de Naciones Unidas, son medidas más que deseables si pretende lograrse la seguridad jurídica en una determinada materia. De este modo, además de conseguir limitar o, incluso, evitar la proliferación de estas armas, pudiera pensarse que la delimitación de su uso, implicaría una definición del hecho ilícito, conforme al Derecho Internacional. Es decir, que la obligación jurídica, cuya contravención origina la exigencia de responsabilidad internacional, quedaría suficientemente definida en una norma explícita.

Sin embargo, pese a los logros alcanzados por los instrumentos jurídicos que han sido citados, no parece que ninguno de ellos contenga un sistema que pudiera ser asumido plenamente para la regulación de las armas cibernéticas, por cuanto, como ya ha sido apuntado, la naturaleza virtual de este armamento y, por lo tanto, su fácil ocultación, dificultaría enormemente un régimen de visitas e inspecciones como los señalados. De este modo, únicamente, confiando en la buena voluntad de los Estados, podría logarse una mínima eficacia en la materia.

Por último, es preciso realizar una breve referencia a la costumbre internacional en esta materia. Así, además de la prohibición de determinados usos de estas armas, acometida por el Derecho Internacional convencional, el DIH consuetudinario recoge, en las Normas 73 y siguientes de la Compilación de DIH Consuetudinario[98], la prohibición de su empleo. En concreto, la Norma 73 prohíbe el empleo de armas biológicas, tanto en los conflictos armados internacionales como en los no internacionales. Esta norma, a tenor de la propia

98 HENCKAERTS, J. M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, vol. I, Normas. Comité Internacional de la Cruz Roja, Buenos Aires (Argentina), 2007; pp. 287 y ss.

Compilación, se aplica a las armas biológicas, diseñadas para atacar a seres humanos. Por otra parte, la Norma 74 prohíbe el empleo de armas químicas, asimismo, tanto en los conflictos armados internacionales como en los no internacionales, al entenderse, en ambos casos, que los Estados no disponen de armamentos distintos en función del carácter internacional o no del conflicto en el que participen. En ambos supuestos, la Norma ha podido establecerse, habida cuenta la ausencia de práctica oficial en contrario.

Sin embargo, en esta tarea que aquí se acomete, por la que se pretende concluir cuál sea el régimen jurídico aplicable a internet, la ausencia de práctica de los Estados, en relación a las ciberarmas, supone un serio obstáculo en la equiparación con las que aquí se vienen examinando. Como señala SHACKELFORD, puede observarse cierto consenso en la condena a determinados tipos de prácticas, llevadas a cabo a través de internet, pero no puede decirse lo mismo, del modo en que ha de responderse. Esa misma ausencia de consenso es puesta de manifiesto por el autor, en relación a la consideración de los supuestos en que un ciberataque puede ser entendido como un ataque armado[99], sin que proceda aquí realizar más análisis de la cuestión, por cuanto ha sido ya tratada en el previamente.

La adopción pues, de un Tratado Internacional que recogiera el concepto de ciberataque como ataque armado, que prohibiera su uso, en aquellos casos que resultan contrarios a la Carta de Naciones Unidas y, a semejanza de lo que ocurre con otras armas de doble uso, instaurara un mecanismo de control y verificación, debería alcanzarse superando no pocos obstáculos. Algunos de éstos podrían provenir de la distinta voluntad de los Estados, derivado de su diverso desarrollo alcanzado. Es obvio que no todos los Estados cuentan con el mismo nivel tecnológico y que ello podría influir en los distintos intereses en cuanto a la materia. Pero, además, hay que tener en cuenta que, incluso, en aquellos ámbitos en los que se ha alcanzado un consenso, que ha permitido contar con un Tratado

99 Esta es la reflexión aportada por SHACKELFORD. El autor propone: «I*n the absence of custom, several treaty regimes may provide bases for the regulation or outright prohibition of cyber attacks in international law*». SHACKELFORD, S. J. *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. Berkeley Journal of International Law. 192, 2009; pp. 193 a 250, en particular, p. 219.

específico que regule determinadas armas, tampoco ofrecen una solución perfectamente acomodable a los supuestos que aquí se contemplan. En efecto, los intentos realizados en orden a conseguir un consenso suficiente que permita la adopción de un Tratado en la materia que limite la proliferación de este nuevo armamento, se han visto seriamente entorpecidos por determinados Estados[100].

Por este motivo, es preciso retomar la segunda de las corrientes apuntadas por el CICR. En consecuencia, es necesario abordar el estudio de la posible aplicación de los principios generales y las normas de DIH, referidas al uso de todos los métodos de combate para atender, de este modo, al "*imperativo de humanidad*".

En consecuencia, hay que volver a recordar que, el daño que, ocasionalmente, pueda causar el lanzamiento de un ciberataque, ha de ser equiparado al que cualquier otro tipo de armamento pudiera originar. Por esta razón, a pesar de que todavía no se han constatado acciones devastadoras, desde el punto de vista humanitario, cometidas empleando armas cibernéticas, es necesario tener presente este principio, a la hora de abordar el régimen jurídico aplicable a este método de combate[101].

Este planteamiento tampoco constituye una completa novedad, pues la aplicación de las clásicas normas, relativas a los métodos de combate, a nuevos tipos de armamento, ha sido ya tratada con anterioridad. Por lo tanto, la aplicación analógica al armamento cibernético resulta obligada, si se pretende dar una respuesta jurídica al uso del mismo.

---

100 Este hecho es puesto de manifiesto, asimismo, por SHACKELFORD, quien apunta: «*International efforts to form a legal regime regarding cyber attacks have been just as happenstance as those aimed at limiting the spread of space weapons. Russia and China have advocated for such a treaty, but the U.S. has demurred. The usual rationale given by the U.S. is that it wants to maintain its space dominance. Similar efforts to cement a treaty for cyber attacks have also failed thus far for the same reasons. As for space weapons, Russia has drafted a resolution calling on nations to ban the development and production of information weapons* ». SHACKELFORD, S. J. *From Nuclear War to Net War,* op.cit.; p. 221.

101 Así se expresó el Comité Internacional de la Cruz Roja, en la 34ª Mesa Redonda celebrada en San Remo, al manifestar: «*So far, we do not know precisely what the humanitarian consequences of cyber warfare could be. It appears that technically, cyber attacks against airport control and other transportation systems, dams or nuclear power plants are possible. Such attacks would most likely have large-scale humanitarian consequences. They could result in significant civilian casualties and damages*». CICR, *International Humanitarian Law and New Weapon Technologies*, doc. cit.

Uno de los ejemplos más paradigmáticos, en relación a las armas de doble uso, se encuentra en el armamento nuclear. En su regulación y tratamiento jurídico, son varios los aspectos a los que es preciso hacer referencia, pues, con la excepción del aludido TNP, a diferencia de las armas químicas y biológicas, las armas nucleares no están explícitamente prohibidas. Por este motivo, constituyen, asimismo, un ejemplo de cómo el Derecho Internacional ha optado por la observancia de los principios generales y las normas aplicables a todos los métodos de combate, atendiendo, así al "*imperativo de humanida*d".

Esta ausencia de regulación expresa convencional, del empleo del armamento nuclear, no ha originado un uso ilimitado del mismo. Al contrario, esta situación provocó que la Asamblea General de las Naciones Unidas decidiera plantear dicha cuestión a la CIJ, en los siguientes términos: "*¿Autoriza el derecho internacional en alguna circunstancia la amenaza o el empleo de armas nucleares?"*. El resultado de la misma se plasmó en la ya citada Opinión consultiva, emitida el 8 de julio de 1996, sobre la legalidad de la amenaza o el empleo de armas nucleares. En dicha Opinión Consultiva, la CIJ concluye que en el Derecho Internacional Convencional no hay una prohibición total y universal, con respecto al empleo de las armas nucleares[102]. Ademas, la Corte establece que "en cuanto a las armas de destrucción masiva, la pauta seguida hasta ahora ha sido declararlas ilícitas en instrumentos específicos". La Corte, como pone de relieve McCORMACK, contrasta la existencia de la Convención sobre las Armas Biológicas y la Convención sobre las Armas Químicas, en la que se establecen prohibiciones generales de las armas biológicas y químicas, respectivamente, «*con el fracaso de la comunidad internacional en imponer una prohibición general de las armas nucleares mediante un convenio sobre armas nucleares*»[103].

La Corte aclaró, asimismo, que, toda vez que ni el Derecho Internacional Convencional ni el Consuetudinario prevén una autorización específica en

102 Un análisis de la citada opinión, puede encontrarse en HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p. 285.

103 McCORMACK, T.L.H., *Un non liquet con respecto a las armas nucleares*. Revista Internacional de la Cruz Roja. 31 de enero de 1997. Disponible en el sitio web: https://www.icrc.org/spa/resources/documents/misc/5tdlba.htm. Fecha de consulta enero 2013.

relación al uso de estas armas, o de la amenaza a través de las mismas, éstos deberían ser, en todo caso, conformes con las exigencias del Derecho Internacional, aplicable en los conflictos armados. Así se expresa la Corte al respecto, cuando, en el párrafo 86 de la Opinión Consultiva, establece:

> "(…) nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the Conferences of 1949 and 1974-1977 left these weapons aside, and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, in the Court's view, it can not be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future. In this respect it seems significant that the thesis that the rules of humanitarian law do not apply to the new weaponry, because of the newness of the latter, has not been advocated in the present proceedings".

Esta conformidad, a juicio de la Corte, debía conseguirse, sobre todo, en relación a los principios y las normas de DIH, así como con las obligaciones concretas en virtud de tratados y otros compromisos referidos específicamente a las armas nucleares. La Opinión Consultiva declara, igualmente, la ilegalidad de recurrir a la amenaza o el empleo de armas nucleares, de forma incompatible con los propósitos de Naciones Unidas y fuera de los requisitos del artículo 51 de la Carta, afirmando que, en todo caso, esa amenaza o empleo de las armas nucleares debe ser compatible con el Derecho Internacional[104] aplicable a los conflictos armados y que existe la obligación de concluir negociaciones tendentes al desarme nuclear total, bajo un estricto y efectivo control internacional[105]. El texto definitivo fue aprobado por ocho votos a favor, frente a siete en contra, si bien, tres de los votos emitidos en contra se justificaron por estar a favor de la total ilegalidad de la amenaza o empleo de las armas nucleares, en toda circunstancia,

104 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996; par. 38

105 *Ibidem*; par. 73.

sin que se pudiera alegar la excepción de «*circunstancias extremas*», contenida en el texto final. Ello supone que, actualmente, sigue sin conseguirse una prohibición del uso de las armas nucleares en cualquier circunstancia[106]. La CIJ concluye que el empleo de las armas nucleares "*es difícilmente conciliable con el respeto de estas exigencias*", pero, aun así, mantiene determinadas reservas, que se justifican por la Corte, afirmando no disponer de "*suficientes elementos para poder concluir con certeza que el empleo de las armas nucleares estaría necesariamente en contradicción con los principios y las normas del derecho aplicable en los conflictos armados en todas las circunstancias*[107]", de tal forma que no puede excluirse la posibilidad de un empleo lícito de las armas nucleares en una "*circunstancia extrema de legítima defensa, en la que esté en juego la supervivencia misma de un Estado*".[108]

Estas conclusiones, sin embargo, no pueden resultar meras declaraciones genéricas, antes bien, pueden y deben materializarse en resultados concretos. De este modo, en aplicación de lo establecido por la CIJ, puede afirmarse que determinadas normas de DIH son de directa aplicación al empleo de las armas nucleares. El uso de las mismas, en los conflictos armados, no puede sustraerse a la regulación de las normas generales de DIH, a través de las que se establecen limitaciones a los métodos de combate y que, asimismo, indican las medidas que han de ser adoptadas en orden a limitar las consecuencias de su uso para la población y las zonas civiles[109].

---

106 Así lo pone de manifiesto, QUEVEDO RUIZ, para quien esta cuestión «*sigue siendo una asignatura pendiente de la comunidad internacional*». QUEVEDO RUIZ, J.R. *Naciones Unidas y la lucha contra la proliferación de las armas,* op.cit; pp. 143 y 144.

107 Legality of the Threat or Use of Nuclear Weapons, doc.cit; par. 95.

108 La opinión Consultiva, ha recibido críticas como la expuesta por McCORMACK, quien entiende que no es aceptable un *non liquet* en esta materia y que el hecho de que «*la mayoría* [de los jueces] *limitara su decisión con respecto a la ilicitud de la amenaza o del empleo de armas nucleares refiriéndose a una "circunstancia extrema de legítima defensa" en vez de argumentar, por ejemplo, que dicha amenaza o dicho empleo no son necesariamente contradictorios con el jus in bello, es tanto una sorpresa como una decepción*». «*la incapacidad de la Corte para pasar de los principios generales a una prohibición sustantiva del empleo de armas nucleares debe ser motivo de preocupación*.» McCORMACK, T.L.H., *Un non liquet con respecto a las armas nucleare*s, op.cit.

109 Así se recoge en el documento elaborado, al respecto, por el CICR. Las normas que el Comité entiende aplicables a estos casos son: la norma que prohíbe los ataques contra personas civiles o bienes de carácter civil; la norma que prohíbe los ataques indiscriminados; la norma de la proporcionalidad en el ataque; la norma sobre la protección del medio ambiente natural y la

No podría ser de otro modo, por cuanto estas normas limitativas constituyen el núcleo del DIH consuetudinario y son, en consecuencia, aplicables en todos los conflictos armados. Dentro de estos límites y normas de general aplicación, el CICR hace expresa referencia a la obligación de observar la proporcionalidad en el ataque. Esta limitación cuenta con el gran inconveniente de que los efectos de un arma nuclear pueden depender de diversos factores y, por ese motivo, existe el riesgo de que no sea posible controlar o limitar algunas consecuencias, como lo exige el DIH. No obstante, resulta incuestionable para el Comité la aplicación, en estos casos, de la norma de proporcionalidad.

En efecto, las dificultades prácticas son evidentes, incluso a la hora de aplicar la distinción entre objetivos civiles y militares, habida cuenta la naturaleza del arma, pero ello no puede justificar que se omita la exigencia de evaluar, previamente, el potencial impacto sobre la población civil en relación con la ventaja militar concreta y directa que se espera obtener.

Así, como se expondrá más extensamente, cuando se haga referencia al contenido de la obligación internacional, la aplicación de las normas de DIH obliga a que, con carácter previo al lanzamiento de un ataque, en el que se vaya a utilizar armamento nuclear o cualquier otro de distinta índole, se calculen los daños que, previsiblemente pueden causarse, de forma directa e inmediata, a consecuencia del ataque. Asimismo, en el caso de las armas nucleares, esta valoración deberá extenderse a los efectos que resulten previsibles a largo plazo y que pudieran derivarse de la exposición a la radiación de la población civil. Ello exige que la conducción de las operaciones militares se realice con la debida protección a la población y bienes de carácter civil, de tal modo que, en el planeamiento de dicha operación, se valoren todas las consecuencias previsibles. De dicho examen podrá concluirse la inoportunidad del empleo de este arma o del lanzamiento de una concreta operación.

La especial idiosincrasia del arma nuclear puede ponerse en parangón, con la que se predica de los ciberataques, de modo que la declaración, anteriormente

---

obligación de tomar las precauciones factibles en los ataques. CICR. *Armas nucleares y Derecho Internacional Humanitario*. Nota informativa número 4. Mayo 2013.

mencionada, realizada por el CICR puede servir de base para aplicar, como se verá con mayor detalle posteriormente, a los ciberataques. Es decir, en ocasiones, la especial dificultad, desde un punto de vista práctico, en el control y manejo de este arma, pudiera llevar a la conclusión de que resulte imposible aplicar determinadas normas de DIH a la guerra cibernética. Sin embargo, resulta obligado defender la postura contraria y abogar por la imperatividad de las normas de DIH que obligue a los Estados a impulsar el correspondiente desarrollo tecnológico y a incentivar los oportunos planes de adiestramiento, que permitan el uso responsable de este arma y que resulte de conformidad con las normas de DIH.

En la misma línea, el propio CICR entiende que la Declaración de San Petersburgo considera aplicables, a los nuevos medios y métodos de combate, determinados principios generales que informan la aplicación del DIH, en tanto un arma no se halle específicamente prohibida[110].

De conformidad con el DIH, tambien están prohibidos los ataques indiscriminados[111] y, en consecuencia, tampoco en el uso de las armas virtuales, se permitiría un ataque de tal índole. Aunque se verá con mayor detalle, puede adelantarse que esta prohibición implica la del uso de armas que no se dirigen o no pueden dirigirse contra un objetivo militar concreto o cuyos efectos no sea posible limitar. La misma reflexión puede aquí realizarse en relación, no sólo a la inexcusable aplicación del DIH a las armas nucleares, que ha quedado taxativamente establecida también por la CIJ[112], sino también en la traslación que aquí se propone, en relación a las ciberarmas. En efecto, tratándose una norma de DIH consuetudinario, no puede evitarse su aplicación en el desarrollo de los conflictos armados, con independencia del tipo de operación que se planifique o

110 Tal afirmación puede encontrarse en el informe resultante de la XXVII Mesa Redonda sobre Problemas Actuales del derecho internacional humanitario. CICR, *El derecho internacional humanitario y los retos de los conflictos armados contemporáneos*, doc. cit.; p. 810.

111 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit; pp. 265-273.

112 La Corte Internacional de Justicia, en la Opinión Consultiva relativa al uso de armas nucleares, declaró que la prohibición de emplear medios y métodos de guerra de tal índole que causasen males superfluos o sufrimientos innecesarios constituye uno de los "*principios cardinales*" del DIH. Legality of the Threat or Use of Nuclear Weapons, doc. cit.; par.78.

del armamento que se pretenda utilizar. Idéntica conclusión alcanza la CIJ, al examinar la norma 71, recogida en la Compilación de DIH consuetudinario y que prohíbe «*el empleo de armas de tal índole que sus efectos sean indiscriminados*»[113] e idéntico razonamiento puede realizarse en relación a su aplicación a las armas cibernéticas[114].

Por ultimo, no puede obviarse, en este planteamiento, la obligatoriedad de la norma relativa a la protección del medioambiente, que obliga a que todos los medios y métodos de guerra sean empleados, teniendo en cuenta la protección y preservación del medio ambiente natural y tomando todas las precauciones factibles para evitar o, al menos, reducir los daños incidentales en el entorno natural[115].

En conclusión, de las exigencias mencionadas se desprende que tanto la amenaza como el empleo de las armas nucleares podrían constituir, con carácter general, un acto contrario a las normas de Derecho Internacional aplicable en los conflictos armados internacionales y, en particular, a los principios y las normas de DIH. Sería, no obstante, deseable alcanzar un consenso en la Comunidad Internacional suficiente, en relación a la práctica común, que evitara la laguna que la referida Opinión declara existente en este tema.[116]En tanto dicho consenso no se alcance y, toda vez que nos encontramos ante una serie de posibilidades de uso de unos materiales, cuyo potencial bélico no ha sido examinado todavía

113 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit; pp. 273-279.

114 Esta misma reflexión, con carácter más extenso, puede encontrarse en VELÁZQUEZ ORTIZ, A.P., *Consideraciones sobre los ciberataques a la luz de los principios generales del empleo de las armas de conformidad con el Derecho Internacional Humanitario*. Seguridad y conflictos: una perspectiva multidisciplinar. VVAA. Miguel Requena (ED). Colección Investigación Instituto Universitario Gutiérrez Mellado.2013; pp.435-463.

115 El artículo 35(3) del Protocolo I adicional a los Convenios de Ginebra 1977 prohíbe el uso de métodos o medios de guerra que hayan sido concebidos para causar, o de los que quepa prever que causen, daños extensos, duraderos y graves al medio ambiente natural. Sin embargo, esta norma no se ha incorporado en el derecho consuetudinario con respecto a las armas nucleares. Asi se contempla en el documento, CICR *Armas nucleares y Derecho Internacional Humanitario*, doc. cit.

116 La Corte, expresamente declara al respecto: "Sin embargo, en vista de la situación actual del derecho internacional y de los elementos de hecho a su disposición, la Corte no puede llegar a una conclusión definitiva sobre si la amenaza o el empleo de las armas nucleares seria licito o ilícito en una circunstancia extrema de defensa propia, en que se viera comprometida la supervivencia misma del Estado". Legality of the Threat or Use of Nuclear Weapons, doc.cit; par. 226.

desde una perspectiva material, ni tampoco jurídica, convendría recordar que el artículo 36 del PA I establece que

> "Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante."

En consecuencia, tomando como referencia la conclusión alcanzada por la CIJ, en su Opinión Consultiva, y las referencias extraidas de la legalidad internacional, pudiera plantearse en qué modo dichos principios y normas resultan de aplicación a las armas cibernéticas.

En el caso que aquí se trata, el examen que se establece en el articulo 36 del PA I, se presenta de un modo especialmente necesario, por cuanto la Comunidad Internacional carece de toda referencia normativa explícita, en relacióna la licitud del uso de este elemento cibernético, a la hora de ser utilizado como método de combate. Esta necesidad puede entenderse compartida por el CICR, cuando expresa que "*efectuar exámenes jurídicos de las nuevas armas reviste particular importancia en la actualidad, debido al rápido desarrollo de las nuevas tecnologías de armas*"[117].

En cualquier caso, el examen de este método de combate deberá realizarse, teniendo en cuenta la imposibilidad de soslayar, por parte de los Estados, el cumplimiento del DIH, cuando se hallen en el transcurso de un conflicto armado. Por otra parte, no hay que olvidar que los Estados están obligados a garantizar "*que se disponga en todo momento de asesores jurídicos que aconsejen a los comandantes militares sobre el DIH y sobre "la enseñanza que deba darse al respecto a las fuerzas armadas*[118]".

Así pues, de la conjunción de ambas disposiciones imperativas para los Estados, se desprende la necesidad de que las Fuerzas Armadas cuenten con una

117 LAWAND, K. *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos Medidas para aplicar el artículo 36 del PA I de 1977*. Comité Internacional de la Cruz Roja Ginebra, enero de 2006. Unidad Armas, División Jurídica; p. 4.
118 De este modo se establece en el artículo 82 del PA I.

formación adecuada que, en las cuestiones de legalidad, deberán confrontar con sus Asesores Jurídicos. De esta manera, los miembros de las Fuerzas Armadas deberán conocer el modo en que los ciberataques pueden ser empleados en el combate, sin contravenir las normas de DIH. El examen previo, a que se refiere el artículo 36 transcrito, ha de comprender, a juicio del CIRC, todas las armas, y así el Comité enumera aquéllas que sean armas "*antipersonal o antimaterial, "letales", "no letales" o "menos letales", y sistemas de armas*[119]".

En este sentido, podríamos encontrarnos con la obligación de dicho examen respecto de los ciberataques, pues, en función del uso que las Fuerzas Armadas del Estado beligerante realizara de ellos, podrían ser encuadradas en todas las categorías enunciadas. No obstante, aun cuando dicho encuadramiento resulte complejo, el CIRC advierte de que este examen previo comprende, asimismo, "*las maneras en que han de utilizarse esas armas conforme a la doctrina militar, las tácticas, las reglas de enfrentamiento, los procedimientos de operación y las contramedidas*[120]". No puede quedar duda, pues, en relación a esta necesidad de evaluación, en relación a los ciberataques, a la vista de la pauta ofrecida por el CICR. En este sentido, adecuar el empleo de los ataques cibernéticos a la doctrina militar de las Fuerzas Armadas en conflicto, así como a sus propias ROE´s[121] constituye una garantía del uso de dichos ciberataques, conforme al DIH.

No finaliza aquí la enumeración ofrecida por el CICR, sino que, además, el Comité añade que, la evaluación impuesta a los Estados por el PA I, comprende, tambien, "*todas las armas que hayan de ser adquiridas, sean armas fabricadas conforme a un proceso de investigación y desarrollo sobre la base de especificaciones militares, o armasen existencia*". En consecuencia, han de entenderse incluidos, en esta última previsión, los métodos cibernéticos, de modo tal que la adquisición y desarrollo,

119 LAWAND, K. *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos*; op.cit; p. 8.
120 *Ibidem*; p. 8.
121 Acrónimo en inglés de Reglas de Enfrentamiento (Rules Of Engagement). Respecto del concepto y naturaleza de dichas Reglas, mucho se ha debatido, sin embargo, a los efectos que aquí atañen, bastará decir que se trata de órdenes que el Mando emite, recogidas en un catálogo y que definen el límite del uso de la fuerza, para cada una de las situaciones que se presenten, en el desarrollo del conflicto armado.

tanto de hardware como de software, destinados a su uso bélico, debería ser evaluada con carácter previo, en orden a determinar su licitud o ilictud.

Por último, concluye el CIRC, imponiendo el examen de las armas de primera adquisición, aunque no sean novedosas, así como de las que ya existen, pero han sido "*modificada(s) de tal manera que se altera su función, o un arma que ya ha sido sometida a un examen jurídico, pero que luego es modificada; un arma existente cuando un Estado se adhiere a un nuevo tratado internacional que puede afectar la licitud del arma*"[122].También en este punto resulta sencillo identificar la necesidad del examen de las ciberarmas. En efecto, en muchos supuestos, los Estados podrán verse en la necesidad de evaluar el empleo de tecnologías, a las que se ha *alterado su función,* hasta el punto de emplear dichas tecnologías con fines bélicos, cuando su configuración originaria no preveía tal modalidad de uso.

El examen, pues, del uso de los ciberataques, así como de la tecnología que los permite, resulta especialmente necesario a la vista de las anteriores previsiones y de la que, adicionalmente realiza el CICR, cuando advierte de que "*un arma que se utiliza de una manera puede "pasar la prueba" del artículo 36, pero puede no pasarla cuando se la utiliza de otra manera*"[123]. Conforme a lo que se ha expresado en los apartados precedentes de este epígrafe, es evidente que la previsión del artículo 36 del PA I y la consiguiente prevención, que realiza el CICR, con carácter general, para todas las armas nuevas, resulta especialmente indicado para las cibernéticas. De hecho, únicamente el modo en que éstas sean utilizadas, llevará a su consideración de arma. Es decir, consecuentemente con la conceptuación realizada como arma de doble uso, sólo si internet se utiliza con las características que han sido descritas, podrá ser entendido como tal. En todos los demás supuestos, internet, simplemente, constituirá un medio de comunicación o transmisión al servicio de las Fuerzas Armadas de un Estado, que podrá y deberá emplearse, en el transcurso de un conflicto armado.

En el momento de proceder al examen al que los Estados vienen obligados en virtud del artículo 36, será preciso analizar la legalidad internacional,

122 LAWAND, K. *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos*, op.cit.; p. 8.
123 *Ibidem*; p. 9.

vinculante para el Estado en cuestión y, en todo caso, "*las normas generales de DIH que se aplican a todas las armas, los medios y los métodos de guerra ya las normas particulares de DIH y de derecho internacional que prohíben el empleo de armas y medios de guerra específicos o que restringen los métodos con los que pueden utilizarse*[124]." Este análisis se tratará con mayor profundidad en el Capítulo siguiente, toda vez que el mismo tiene por objeto el examen del contenido de la norma internacional infringida. En cualquier caso, pueden abordarse los aspectos que han de ser cuestionados por los Estados, con la asistencia del Asesor Jurídico de las Fuerzas Armadas, a la hora de determinar la licitud o ilicitud del método de combate.

En el ámbito que nos ocupa, tan relevante resulta la obligación a la que el Estado se halla vinculado, en virtud de Derecho Internacional Convencional, como la surgida del Derecho Consuetudinario. Es decir, que el estudio de licitud del método de combate, deberá contemplarse a la luz de ambos. Ya se ha podido comprobar cómo, en los casos en que el Derecho Internacional Convencional no ha podido dar respuesta al empleo de nuevas armas, como el caso del armamento nuclear, ha sido la aplicación del Derecho Consuetudinario la que ha provisto de unos parámetros, que no pueden ser ignorados. En el caso de los ciberataques, vista la indefectible aplicación del DIH al elemento cibernético, no cabe duda de que la Compilación de DIH Consuetudinario recoge normas que son de obligada observancia, en el lanzamiento de ataques cibernéticos, como también se verá más adelante.

Por otra parte, también resulta evidente que, en ausencia de cualquier otro criterio aplicable, los principios de humanidad y la conciencia pública están llamados a arrojar luz sobre el tema, como pone de manifiesto el CICR, cuando indica que, en los supuestos en que ninguna de las normas citadas, de origen convencional o consuetudinario, cuenten con una específica previsión del medio o método de combate sometido a examen, será preciso "*considerar el arma propuesta a la luz de los principios de humanidad y los dictados de la conciencia pública*[125]". Es decir, que dicho análisis, concluye con la invocación de la llamada

124 *Ibidem*; p.9.

125 Esta consideración se justifica en la previsión de la misma contemplada en el artículo 1(2) del PA I, el preámbulo del Convenio IV de La Haya relativo a las leyes y costumbres de la guerra

"cláusula de Martens", que el artículo 1(2) del PA I enuncia de la siguiente manera:

> "En los casos no previstos en el presente Protocolo o en otros acuerdos internacionales, 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".[126]

Nuevamente, se hace necesario retomar las directrices ofrecidas por la CIJ en su Opinión Consultiva, emitida a resultas del examen de licitud de las armas nucleares. En dicha Opinión Consultiva, la CIJ realizó una expresa referencia a estos principios de humanidad y conciencia pública, en los siguientes términos:

> "The Court would likewise refer, in relation to these principles, to the Martens Clause, which was first included in the Hague Convention II with respect o the Laws and Customs of War on Land of 1899 and which has proved to be an effective means of addressing the rapid evolution of military technology."[127]

Sería deseable, incluso, que estos principios no quedaran relegados a ser una última solución, aplicable, únicamente, a falta de las demás, sino que también fueran tenidos en cuenta, como criterios interpretativos de las normas convencionales y consuetudinarias, en el caso de que estas se aplicaran.

En cualquier caso, el examen impuesto por el PA I, realizado a tenor de las directrices que han sido expuestas, resultaría de gran utilidad para las Fuerzas Armadas de los Estados que, en el desarrollo del combate, pretendieran hacer uso de este nuevo método. No se trata aquí de realizar un estudio teórico o hipotético, sino, antes bien, de alcanzar una serie de conclusiones que faciliten el manejo de este método por quienes van a estar al mando de las operaciones, en las que se utilice. Dichas conclusiones, por otra parte, se hacen todavía más

---

terrestre, 1907 y el preámbulo de la Convención II de La Haya de 1899 relativa a las leyes y usos de la guerra terrestre y reglamento anexo.

126 LAWAND, K. *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos*, op.cit.; p. 14.

127 Legality of the Threat or Use of Nuclear Weapons, doc.cit.; par. 78.

necesarias cuando, como se verá a continuación, un ciberataque puede constituir un hecho ilícito, incluso cuando se realice como consecuencia de una omisión.

La determinación de la licitud del armamento cibernético y de su modo de empleo debería constituir el primer paso a dar, en orden a garantizar el adecuado conocimiento del mismo. Tampoco esta cuestión resulta superflua o gratuita; antes bien, constituye el resultado del cumplimiento de las normas que, sobre adiestramiento, aparecen, expresamente contempladas, en DIH. De este modo, los Estados deberían poner especial énfasis en valorar si el uso de sus equipos y programas informáticos, durante el combate, se ajusta a las previsiones de DIH, lo que debería realizarse desde el mismo momento, en que ese material físico o virtual fuera adquirido o desarrollado. De la misma manera que los Estados han demostrado un creciente interés por protegerse frente a ciberataques, a través de la creación de unidades militares específicas[128], deberían acudir al examen contenido en el articulo 36 del PA I y a los criterios establecidos por el CICR, para concluir en qué modo dicho método puede ser utilizado por ellos, sin contravenir las obligaciones internacionales, que serán expuestas más adelante.

4. EL HECHO ILÍCITO COMETIDO POR ACCIÓN.

Una vez sentadas las bases que constituyen la conceptuación de un ciberataque como ataque armado, así como la legalidad internacional de aplicación al mismo, resulta necesario plantearse si un ciberataque puede constituir un hecho ilícito, al incumplirse una obligación internacional de DIH, que genere responsabilidad internacional del Estado autor del referido hecho.

El uso de la red, bien en el inicio de un combate, bien durante el desarrollo del mismo, presenta ciertas dudas sobre el modo en que aquélla puede y debe ser

128 Un ejemplo de ello lo constituye en España el citado MCCD. La propia Exposición de Motivos de la Orden Ministerial de su creación resalta la necesidad contar con la disposición de capacidades adecuadas y la determinación de utilizarlas, si fuera necesario. En consecuencia, prevé que el Ministerio de Defensa participe en el impulso de una gestión integral de la ciberseguridad, en el marco de los principios que se establezcan al efecto en la Estrategia de Ciberseguridad Nacional. Sobre las funciones del MCCD, así como su regulación jurídica, puede consultarse AMICH ELIAS, C. y VELAZQUEZ ORTIZ, A.P. *La ciberdefensa y sus dimensiones global y específica en la Estrategia de Seguridad Nacional*, en Revista ICADE, núm. 92 (Monográfico dedicado a: Seguridad y Defensa. Reflexiones a la luz de la Estrategia de Seguridad Nacional 2013); mayo-agosto 2014; pp. 49-76.

utilizada. En cualquier caso, resulta obvio que su empleo se presenta como deseable en determinadas situaciones y que es previsible un aumento en el uso de este tipo de medios de combate. Ciertamente, el avance tecnológico ofrece indudables ventajas, pues es evidente que «*Los robots no se descontrolan en el calor de la batalla, ni tienen estrés ni se deprimen. No actúan por ira, venganza, prejuicio o temor, ni causarán daños innecesarios a la población civil, no torturarán ni violarán*»[129]. Si bien esta afirmación hace referencia a una distinta modalidad de método de combate, como son los llamados drones, no puede dejar de compartirse el mensaje ínsito en ella, pues el uso de métodos de combate que permiten una precisa programación, debería ofrecer la posibilidad, asimismo, de un mejor cumplimiento de las normas aplicables al combate.

Por otra parte, como también se ha puesto de manifiesto,

> "(…) estas ventajas de los robots militares cambiarán también la consideración de la guerra como "extensión de la política". Los LAR[130] reducirán el coste humano de los conflictos armados llevando a la normalización de los conflictos. Esto puede tener el efecto de bajar el umbral de entrada en guerra para los Estados y de que la guerra no sea una opción de último recurso"[131].

Sin embargo, no puede obviarse que la esa misma tecnología, usada en el modo que ya se ha visto en los apartados precedentes, puede originar acciones u omisiones que constituyan un hecho ilícito.

Así las cosas, la cuestión será identificar las obligaciones convencionales o consuetudinarias, susceptibles de ser infringidas por un Estado, a la hora de lanzar un ciberataque, en un conflicto armado internacional o no internacional. En un principio, la aplicación del DIH a los ciberataques, tal y como ha quedado expuesta, conlleva que las normas de DIH no pueden quedar al margen de dicha observancia. Por otra parte, tampoco puede dejar de tenerse en cuenta que el ilícito internacional se producirá cuando resulta violada una obligación internacional, «*sea cual fuere el origen o la naturaleza de esa obligación*», es decir, con

129 Actualización de Internet II Metafísica. Centro de Análisis y Prospectiva. Gabinete Técnico de la Guardia Civil. Boletín actualidad internacional. Abril-Mayo 2015; p. 27.
130 Acrónimo en inglés de Robots Autónomos Letales.
131 Actualización de Internet II Metafísica, doc. cit.; p. 27.

independencia de que el origen de la misma, sea convencional o consuetudinario[132].

Sin embargo, es esencial abordar la cuestión de si el Proyecto resulta de aplicación a las normas convencionales y consuetudinarias que conforman el DIH. No puede entenderse superficial este planteamiento, pues, como plantea SASSOLI, « *¿No es acaso el derecho internacional humanitario un "sistema autónomo" que debe aplicarse sólo de conformidad con sus propias normas*?» Este concepto de sistema autónomo, equiparado al que rige en el ámbito del Derecho Diplomático, ha sido, finalmente, abandonado por la propia CDI, incluso para las relaciones diplomáticas[133].

En consecuencia, este nuevo planteamiento, obliga a una reflexión acerca del llamado carácter autónomo del DIH, lo que obliga a plantearse la cuestión de si el DIH puede aplicarse, únicamente, mediante los mecanismos que el mismo establece, explícitamente. Como punto de partida de dicha reflexión, SASSOLI recuerda quedan expresamente prohibidas las contramedidas, consistentes en conductas que afecten a las víctimas de la guerra:

> "(…) estos mecanismos detallan o modifican normas generales sobre la responsabilidad del Estado que sólo pueden comprenderse en ese marco y, por otra parte, los tribunales internacionales han aplicado normas generales sobre la responsabilidad del Estado para atribuir o no ciertas violaciones del derecho internacional humanitario a un Estado en particular"[134].

Sin perjuicio de las consideraciones que se harán en torno a las contramedidas y su diferenciación de las represalias bélicas, en el capítulo cuarto, ha de tomarse esta referencia como indicio de la posible autonomía del DIH respecto del sistema de responsabilidad internacional del Estado, instaurado por el Proyecto. Es decir, podría plantearse la cuestión de si el DIH contiene un

132 Comentario al artículo 12 del Proyecto de artículos.

133 Asi lo plantea el autor en SASSÒLI, M., *La responsabilidad del Estado por las violaciones del Derecho Internacional Humanitario*. Revista Internacional de la Cruz Roja. Junio 2002. Documento disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/5tecbx.htm. Fecha de consulta, octubre de 2013.

134 SASSÒLI M., *La responsabilidad del Estado por las violaciones del Derecho Internacional Humanitario*.op. cit.

mecanismo autónomo de responsabilidad y, en consecuencia, de si puede ser exigida dicha responsabilidad, al margen de este mecanismo propio. En relación a esta cuestión, la doctrina internacionalista ha sostenido de modo indubitado que, en efecto, la violación de normas de DIH origina la responsabilidad del Estado que las infringe, conforme a lo dispuesto con carácter general. Así, por ejemplo, BOLLO AROCENA entiende que "*aun cuando el Derecho Internacional Humanitario se rige por algunas reglas propias (5), no es un sistema enteramente autónomo y necesita de los mecanismos generales de aplicación del Derecho Internacional*" [135] .

La contravención de las obligaciones relativas a las normas de DIH, exigibles en el desarrollo del combate, ocasionará la exigencia de responsabilidad internacional del Estado. Como se verá más adelante, en el Capítulo correspondiente al análisis del contenido de la obligación de DIH las limitaciones introducidas por el DIH, a la conducción de operaciones o al empleo de determinados métodos de combate, no ofrece dudas cuando dichos métodos de combate son convencionales, es decir, los comúnmente conocidos hasta ahora. Pues bien, en el uso de internet como método de combate, la solución deberá ser la misma. A la luz de las conclusiones antes alcanzadas, el hecho de que un ciberataque pueda ser considerado un ataque armado, equipara a éste con otros métodos de combate hasta ahora analizados por la doctrina internacionalista y por la Jurisprudencia internacional. Por otra parte, visto que a dichos ataques informáticos ha de serles de aplicación el DIH, su licitud quedará supeditada a la observancia de las limitaciones impuestas por el DIH.

En el análisis de la cuestión que ahora se plantea, es preciso determinar quiénes son los sujetos de Derecho Internacional concernidos por el DIH y, por lo tanto, obligados a dicho cumplimiento. A través de dicho análisis podremos llegar a establecer si nos encontramos ante una obligación internacional, vinculante para todos los Estados, así como si dicha obligación puede oponerse, igualmente, a todos ellos. También en este ámbito, la respuesta requiere una

135 BOLLO AROCENA M. D., *La responsabilidad internacional del Estado por la violación del Derecho Internacional Humanitario. A propósito de los hechos ocurridos en la cárcel de Abu Ghraib (Iraq)*. Revista de Derecho Militar núm. 86 Julio - Diciembre 2005, pp. 153 a 195, en particular, p. 155.

reflexión que abarque los precedentes históricos de la cuestión pues, como pone de manifiesto CARDONA LLORENS, el punto de partida, en este ámbito, lo constituye un concepto unitario del régimen de la responsabilidad internacional.[136]

Dicha postura, aceptada tradicionalmente por la jurisprudencia internacional, tuvo como consecuencia, a juicio del mismo autor, «*la negación de la existencia de normas universales*[137]». Se trataba de un planteamiento, por lo tanto, en el que «*todo Estado tiene derecho a que una norma internacional sea respetada, pero no tiene derecho a que el conjunto del DI y las obligaciones que comporta, sean respetadas en sí mismas*[138]».

Sin embargo, esta tesis fue abandonada por la doctrina y Jurisprudencia internacionales, de forma tal que, en el fallo del caso relativo a la "Barcelona Traction" la CIJ advirtió de que, en esta materia, nos encontramos ante normas *erga omnes*[139]:

> "When a State admits into its territory foreign investments or foreign nationals, whether natural or juristic persons, it is bound to extend to them the protection of the law and assumes obligations concerning the treatment to be afforded them. These obligations, however, are neither absolute nor unqualified. In particular, an essential distinction should be drawn between the obligations of a State towards the international community as a whole, and those arising vis-à-vis another State in the field of diplomatic protection. By their very nature the former are the concern of all States. In view of the importance of the rights involved, all States can be held to have a legal interest in their protection; they are obligations erga omnes".

136 Al respecto, CARDONA LLORENS afirma que "(…) *tradicionalmente la doctrina ha sido casi unánime en considerar que las reglas de Derecho Internacional general relativas a la responsabilidad de los Estados, sólo preveían un régimen único de responsabilidad, aplicable a todas las hipótesis de hechos internacionalmente ilícitos del Estado, cualquiera que fuera el contenido de la obligación contra la que atentara ese hecho y, consistente en la obligación de reparar el daño causado*". CARDONA LLORENS, J. *La responsabilidad internacional por violación grave de obligaciones esenciales para la salvaguarda de intereses fundamentales de la comunidad internacional. (EL «CRIMEN INTERNACIONAL»)*. Anuario de derecho internacional. VIII; pp., 265 a 336, en particular, pp. 270 y 271.
137 Ibidem; p. 272.
138 Ibidem; p. 272.
139 Barcelona Traction, Light and Power Company, Limited, Judgment, I.C.J. Reports 1970; par. 33.

También, con posterioridad, se volverá sobre los efectos *erga omnes* de las normas de DIH, al analizar el posible carácter imperativo de las mismas, pero ahora, puede adelantarse que el citado fallo recoge, asimismo, la naturaleza de *ius cogens* de determinadas normas, entre las que se ha pretendido ver a las que conforman el DIH.[140]

La práctica de los Estados, en relación con las limitaciones impuestas por el DIH a la conducción de hostilidades y al empleo de determinados métodos de combate, ha sido constatada, reafirmando, de este modo, su carácter de normas de efectos frente a todos. Del mismo modo, puede afirmarse que ha sido probada la convicción de dichos Estados de estar actuando en el cumplimiento de una obligación jurídica. Por lo tanto, puede concluirse que ambos elementos configuradores de la costumbre internacional se hallan presentes. Por lo tanto, podemos asegurar que nos encontramos ante una costumbre internacional, entendida como "*prueba de una práctica generalmente aceptada como derecho*[141]". Como se verá en el Capítulo concreto relativo al contenido de la obligación internacional violada, esta definición puede aplicarse a las principales normas que rigen las limitaciones impuestas al combate.

Por último, la caracterización de las normas de DIH como normas *erga omnes*, vinculantes para todos los Estados y frente a todos ellos, encuentra su justificación, en la actualidad, a juicio de CARDONA LLORENS, en la Carta constitutiva de la Organización de Naciones Unidas. Dicho Tratado, a juicio del autor, al enunciar «*los propósitos de la organización, configura unos valores que empiezan a considerarse en sí mismos, al margen de consentimiento individualizado de cada uno de los Estados*[142]». En consecuencia, también a partir de este momento, puede afirmarse la necesidad de normas que, «*salvo pacto expreso en contrario, se apliquen a la generalidad de esos miembros de esa comunidad. Este paso, en una sociedad carente de un órgano legislador universal, debía ser necesariamente, como así está siendo,*

140 Ibidem; par. 34.
141 Así se define por el artículo 38 del Estatuto de la Corte Internacional de Justicia. Anexo a la Carta de Naciones Unidas.
142 CARDONA LLORENS, J. *La responsabilidad internacional por violación grave de obligaciones esenciales p a r a la salvaguarda de intereses fundamentales de la comunidad internacional*, op.cit; p. 274.

a través de la costumbre[143] », entendida, tal y como propone JIMÉNEZ DE ARECHAGA, como «*el resultado del consenso general, no del consentimiento, expreso o tácito, de un Estado en particular (...).No hace falta el asentimiento específico del demandado; lo que el Tribunal tiene que determinar es si, como dice el art. 38 del Estatuto, cierta práctica está "generalmente aceptada como derecho"*[144]».

De conformidad con lo anterior, ha de concluirse que, en relación con el caso que nos ocupa, resulta plenamente aplicable el DIH Consuetudinario. Es en este punto, de especial interés, en el que hay que atender al contenido de la Norma 139 de la Compilación de DIH consuetudinario que establece que «*Las partes en conflicto deberán respetar y hacer respetar el derecho internacional humanitario por sus fuerzas armadas, así como por otras personas y agrupaciones que actúen de hecho siguiendo sus instrucciones o bajo su dirección o control*»[145]. La Norma transcrita recoge, así, la teoría doctrinal anteriormente expuesta, por cuanto entiende que «*la obligación de los Estados de respetar el DIH, forma parte de su obligación general de respetar el derecho internacional*», expresada en los Convenios de Ginebra de 1929 y 1949.

En conclusión, no parece que cause controversia la exigencia de responsabilidad internacional al Estado que viole una norma de DIH, como ya se ha expuesto, y como pone de manifiesto la doctrina internacionalista, de modo indubitado. En consecuencia, puede afirmarse, con BOLLO AROCENA, que la violación de las normas de DIH conlleva la exigencia de responsabilidad internacional[146].

---

143 Ibidem; p.275.

144 JIMÉNEZ DE ARECHAGA, *La costumbre como fuente del Derecho Internacional*, en Estudios de Derecho Internacional en Homenaje al profesor Miaja de la Muela. Tecnos. 1979. Madrid, vol. I, pp. 375-402, en particular; pp. 397-398.

145 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit; p.559.

146 Así se ha manifestado BOLLO AROCENA con ocasión de los métodos empleados en la prisión de Abu Graib, de los que la autora colige la exigencia de responsabilidad internacional a EEUU por los mismos. En este sentido, BOLLO AROCENA entiende que los hechos acaecidos en la prisión de Abu Ghraib, a consecuencia de las violaciones de derechos humanos que pudieran constituir el elemento objetivo de los hechos internacionalmente ilícitos que allí se cometieron y que las obligaciones de DIH, de imperativa observancia que allí fueron infringidas, son las recogidas, esencialmente, en la III Convención de Ginebra de 1949. Asimismo, la autora manifiesta que las prácticas, en contra de las mismas, pueden llegar a originar responsabilidad internacional. Pues bien, concluye afirmando que numerosas prácticas seguidas en Abu Ghraib

Por lo tanto, aun cuando, como se ha anunciado, será motivo de análisis más detallado en el Capítulo Segundo, conviene aquí realizar una sucinta aproximación a la aplicación de esta construcción doctrinal y su correlativa previsión jurídica a los ciberataques. Si ha podido concluirse que el DIH convencional y consuetudinario resultan de obligada observancia para los Estados inmersos en un conflicto armado internacional o no internacional, que utilicen los ciberataques como método de combate es ahora preciso enunciar, las específicas normas a las que el Estado queda constreñido.

Puede afirmarse, que un ciberataque que no responda a una necesidad militar constatada, dará lugar a la violación de obligaciones de DIH. Igualmente, el DIH impone que un ataque armado respete el principio de distinción entre objetivos civiles y militares; limitación que resulta, también, aplicable al conflicto que se libre por medios cibernéticos o haciendo uso de ellos, en combinación con los métodos de combate tradicionales. En el supuesto, pues, de que un ataque cibernético se dirija a un objetivo civil, que no hubiera perdido su condición de no combatiente, nos encontraríamos ante la violación de la obligación internacional consistente en la distinción entre combatientes y no combatientes. Asimismo, tanto el DIH convencional como el consuetudinario exigen que el ataque resulte proporcional a la necesidad militar. La proporcionalidad de los medios empleados y la previa obligación de comprobar las consecuencias de dicho ataque, al objeto de minimizar los daños causados, constituyen una nueva obligación internacional, cuya violación dará lugar a la exigencia de responsabilidad. La prohibición del uso de perfidia, nuevamente, determina la existencia de una obligación internacional que, al igual que las anteriores, se recoge en las normas convencionales y consuetudinarias de DIH, cuya violación dará lugar a la existencia de un hecho ilícito, de conformidad con lo dispuesto en el artículo 2 del Proyecto. Por último, la actuación del Estado que, en el desarrollo de un conflicto, viole la neutralidad de un tercero, a través de una ciberoperación, será objeto, igualmente, de exigencia de responsabilidad respecto del mismo.

---

contravinieron abiertamente algunas de las disposiciones que acabamos de transcribir, tal y como puso de relieve el equipo investigador del CICR. BOLLO AROCENA, M. D., *La responsabilidad internacional del Estado por la violación del Derecho Internacional Humanitario*, op.cit; p. 158.

De forma reiterada se ha puesto de manifiesto la dificultad implícita en el uso del método de combate que se examina. Esta dificultad no reside únicamente en su manejo, sino que se traslada, asimismo, a aspectos tales como la indagación de la autoría del ciberataque y a la ubicación física del atacante. Sin embargo, ello no puede ser óbice para que a los Estados les sea obligado respetar las normas de DIH, pues «*La violación de una obligación internacional constituye un hecho ilícito, cualquiera que sea el objeto o contenido de la obligación violada y cualquiera que sea la descripción que pueda darse del comportamiento que la incumple*.» como se recoge en el Comentario de la CDI al artículo 12 del Proyecto.

Tampoco el hecho de que, en un conflicto armado se combine el empleo de medios cibernéticos con otros que impliquen la fuerza cinética, como se verá más adelante, no puede impedir la aplicación del DIH. Asimismo, dicha aplicación será exigible también en el caso de que el conflicto sea exclusivamente cibernético.

Es decir, si retomamos los ejemplos que se ha ido manejando al atender a las cuestiones anteriormente analizadas, encontramos que el lanzamiento de un virus como Stuxnet podría dar lugar a la consideración del mismo como un hecho ilícito internacional, si, a través del mismo, se llegara a infringir, cualquiera de las normas de DIH que, con carácter enunciativo, se hanmencionado. En este supuesto, aunque se hubiera apreciado la necesidad militar en el lanzamiento de un virus de tal magnitud y complejidad, podría darse el caso de que éste se propagara incontroladamente. La obligación de distinción, pues, entre combatientes y no combatientes, podría verse vulnerada con un ciberataque como el referido. En este supuesto, desde el momento en que dicho lanzamiento fuera atribuido a la acción de un Estado, nada impediría exigir a éste responsabilidad internacional por parte del Estado afectado.

No puede tampoco obviarse, finalmente, que dicha atribución podrá realizarse respecto de un Estado, en función del comportamiento de quienes actúen en su nombre.

Por último, procede hacer referencia al hecho de que, en el ámbito que aquí se expone, será muy frecuente que los Estados no actúen de forma individual. Antes bien, la actuación en un conflicto armado, podrá desarrollarse

en el seno de una Organización internacional o de una coalición de Estados y no resulta impensable que los ataques cibenéticos se presten como una forma de apoyo por parte de otro Estado. En estos casos, no podrá obviarse la previsión que realiza el artículo 16 del Proyecto que declara la existencia de responsabilidad internacional del Estado que presta apoyo cuando se dan las circunstancias siguientes:

> "El Estado que presta ayuda o asistencia a otro Estado en la comisión por este último de un hecho internacionalmente ilícito es responsable internacionalmente por prestar esa ayuda o asistencia si: a) Lo hace conociendo las circunstancias del hecho internacionalmente ilícito; y b) El hecho sería internacionalmente ilícito si fuese cometido por el Estado que presta la ayuda o asistencia".

Pues bien, es en éste último caso donde tendrá que tenerse más presente la norma que acaba de ser expuesta. En esos supuestos, donde cualquier ayuda recibida por el Estado infractor dará lugar a responsabilidad internacional del cooperante. En adelanto al examen que se realizará al atender las cuestiones relativas a la atribución del hecho ilícito, puede señalarse que el Comentario al artículo 16 del Proyecto revela qué ha de entenderse en esas situaciones por "*ayuda o asistencia*" y así, por ejemplo, el hecho de proporcionar "*a sabiendas, un elemento esencial*", entraría dentro de este concepto.

En el contexto que aquí se examina, ese elemento esencial podría suponer la puesta a disposición de un programa o equipos informáticos o bien, de personal especialmente cualificado para su manejo y nada evitaría que, a través de dichos recursos materiales o humanos, se contribuyera de forma esencial a la violación de la obligación internacional, en la que el Estado que recibe la asistencia haya incurrido. En estos supuestos, la exigencia de responsabilidad del Estado que presta la ayuda, como se verá, estará limitada conforme a los criterios expuestos en el Comentario de la CDI. De este modo, la responsabilidad internacional del Estado que asiste al infractor se dará cuando el primero conozca las circunstancias en las que el infractor está actuando, su ayuda sea efectivamente prestada y facilite la comisión del hecho ilícito y, por último, el hecho cometido hubiera sido igualmente ilícito, de haberlo realizado "*el propio*

Estado que presta la asistencia". Por lo tanto, en el ejemplo anterior, nada impediría exigir responsabilidad al Estado que, a sabiendas de que se está atacando una red informática de uso civil presta al Estado atacante un programa informático que facilita dicho ataque y "*contribuye significativamente*" a ello, en el sentido recogido en el párrafo 5 del Comentario al artículo 16 del Proyecto.

5. EL HECHO ILÍCITO COMETIDO POR OMISIÓN.

Si la violación de una obligación internacional, a través de la conducta activa de un Estado, no parece causar ninguna duda, hay que plantearse ahora si esa misma violación puede ser cometida por omisión. Para determinar si, en efecto, el hecho ilícito del Estado, en el empleo de ciberataques es o no viable, es preciso acudir, en primer lugar, a las fuentes convencionales de DIH y, así, traer aquí el texto del artículo 91b) del PA I, que establece que el Estado es responsable de "*todos los actos cometidos por las personas que hagan parte de su fuerza armada*".

La Norma149 de la Compilación DIH advierte que un Estado es, también, responsable de las omisiones de sus órganos, cuando éstos tienen el deber de intervenir, como en el caso de los jefes militares y otros superiores, que tienen la responsabilidad de prevenir los crímenes de guerra y castigar a los culpables.[147]

En consonancia con lo anterior, procede señalar que artículo 2 del Proyecto recoge, expresamente, la posibilidad de que un hecho ilícito internacional consista en "*una acción u omisión*". De igual modo, el Comentario al artículo 2 del citado Proyecto considera completamente factible tal posibilidad, equiparando la omisión a la conducta activa del Estado[148].

---

147 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; pp. 599-606. La citada Norma 149, expresamente al respecto: "*Un Estado es responsable de las violaciones del derecho internacional humanitario que le son imputables, en particular:*

a) las violaciones cometidas por sus órganos, incluidas sus fuerzas armadas;

b) las violaciones cometidas por personas o entidades autorizadas a ejercer prerrogativas de su autoridad gubernativa;

c) las violaciones cometidas por personas o grupos que actúan de hecho obedeciendo sus instrucciones o bajo su dirección o control; y

d) las violaciones cometidas por personas o grupos privados que él reconoce y acepta como comportamiento propio".

148 Así puede leerse en el Comentario 9) al artículo 2 del Proyecto, donde no se hace distinción alguna entre que el incumplimiento de la obligación internacional del Estado, sea cometida por acción o, por ejemplo, a través del incumplimiento de la obligación de promulgar una norma. Es

Asimismo, la Jurisprudencia internacional, tradicionalmente, ha entendido equiparable la omisión a la acción, como conducta susceptible de constituir un hecho ilícito, por el que pueda exigirse responsabilidad internacional al Estado. Así pudo constatarse, por ejemplo, en el asunto de las *Reclamaciones en la zona española de Marruecos,* en 1925, donde quedó establecido que un Estado que no haya ejercido la debida diligencia para evitar o sancionar los actos ilícitos de grupos armados, puede ser considerado responsable de esa omisión. En este caso, el Tribunal determinó que:

> "(…) Toutefois, elle n'exclut point la thèse suivant laquelle il faut assimiler à l'action volontaire l'inaction des pouvoirs publics dans des situations où, en vertu de la mission qui leur est confiée, ils sont appelés à protéger les droits des étrangers et où, en l'espèce, ils sont en état de ce faire. Cela est surtout vrai si les pouvoirs publics ont été avertis d'un danger menaçant les étrangers, ou si le gouvernement du pays dont le damnifié est ressortissant a demandé l'intervention des pouvoirs publics du lieu".

En conclusión,

> "(…) la responsabilité de l'État peut être engagée dans les situations en question, non seulement par un manque de vigilance dans la prévention des actes dommageables, mais aussi par un manque de diligence dans la poursuite pénale des fauteurs, ainsi que dans l'application des sanctions civiles voulues. (…) La responsabilité de l'État en cette matière se trouve certainement engagée, contrairement à l'opinion soutenue par le Représentant espagnol, aussi en dehors de l'obligation de ne pas entraver l'opération de la justice pénale"[149].

Por otra parte, también puede ser tenido en cuenta el asunto *Essen Lynching*, sometido al Tribunal Militar británico de Essen, puede, asimismo, ser tenido en cuenta, como ejemplo de la equiparación de la conducta activa y omisa pues, en dicho proceso, los miembros de la escolta militar alemana resultaron condenados, como consecuencia de su incumplimiento de la obligación a la que

---

decir, el incumplimiento de la obligación del Estado, relativa a promulgar una determinada norma, en el ámbito interno, daría lugar a responsabilidad internacional de Estado, cuando dicho deber venga impuesto por unaobligación internacional.

149 Affaire des biens britanniques au Maroc espagnol Recueil des Sentences Arbitrales. Affaire des biens britanniques au Maroc espagnol (Espagne contre RoyaumeUni) 1er mai 1925. (II), pp. 642 a 646; par. 3 a 6.

se hallaban sujetos, consistente en ofrecer protección a los prisioneros de guerra aliados. Como consecuencia de dicha omisión, los prisioneros fueron objeto de una agresión por la muchedumbre[150].

La posibilidad de la comisión por omisión quedó, asimismo, avalada por la decisión relativa al estrecho de Corfú, en la que se acreditó responsabilidad por omisión de Albania, por su incumplimiento de la obligación de avisar a terceros Estados[151]. Textualmente, en el fallo se establece que,

> "The obligations incumbent upon the Albanian authorities consisted in notifying, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in warning the approaching British warships of the imminent danger to which the minefield exposed them. Such obligations are based, not on the Hague Convention of 1907, No. VTII, which is applicable in time of war, but on certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war; the principle of the freedom of maritime communication; and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.
>
> In fact, Albania neither notified the existence of the minefield, nor warned the British warships of the danger they were approaching. But Albania's obligation to notify shipping of the existence of mines in her waters depends on her having obtained knowledge of that fact in sufficient time before October 22nd; and the duty of the Albanjan coastal authorities to warn the British ships depends on the time' that elapsed between the moment that these ships were reported and the moment of the first explosion".

Así pues, es evidente que el hecho ilícito puede ser cometido por omisión, de tal forma que la ausencia de actuación estatal origine la violación de una obligación internacional.

Si llevamos estas conclusiones al ámbito que nos ocupa, no resulta ocioso plantear la cuestión de cuál es el deber del Estado en relación con el uso de

150 Entre los hechos probados recogidos en la dicha sentencia, puede leerse: (…) *Heyer had ordered the escort not to interfere in any way with the crowd if they should molest the prisoners was proved in evidence, and was also admitted by Heyer himself. It was confirmed by some German witnesses, though not admitted by Heyer, that the made remarks to the effect that the airmen ought to be shot or that they would be shot.*" The Essen Lynching Case TriaL of Erich Heyer and six others British Military Court For The Trial Of War Criminals, Essen, 18th-19th and 21 st-22nd, December, 1945; p. 88.
151 Corfu Channel case, Judgment of April 9th, 1949. I.C.J. Reports 1949; par. 4.

internet, de manera que la ausencia de actuación del mismo pueda originar la responsabilidad que aquí se trata. Nos encontramos, nuevamente, ante el planteamiento de cuestiones novedosas que, si bien, no pueden obviar la argumentación expuesta, sin embargo, no encuentran, exclusivamente en ella, una respuesta adecuada. De este modo, cabrá cuestionarse en qué medida el Estado ha de ser responsable de ofrecer la necesaria ciberseguridad, de modo tal que un ciberataque pueda ser evitado o, al menos minimizado, hasta el punto de no ocasionar una agresión en el sentido expuesto en los apartados anteriores.

En este punto, es preciso volver al examen de la Norma 139 de la Compilación de DIH Consuetudinario, en tanto que la misma alude artículo 1 común a los Convenios de Ginebra de 1949. Este artículo añade la obligación de hacer respetar el DIH y la misma puede encontrase, igualmente, en el PA I. Tal como se formula dicha obligación en la citada Compilación, la misma impone que los Estados «*deben hacer que lo respeten [el DIH], otras personas o agrupaciones que actúen de hecho siguiendo sus instrucciones o bajo su dirección o control*»[152].

En estrecha relación con la Norma transcrita, se encuentra la Norma 149 de la misma Compilación, que atiende a los supuestos en que un Estado es responsable de las violaciones del DIH que le son imputables, sin hacer distinción entre las violaciones de DIH que puedan cometerse, empleando un medio activo u omisivo[153].

Como ya se ha expuesto, la obligación de respetar y hacer respetar el DIH puede entenderse como una obligación *erga omnes* y, por lo tanto, en ningún caso, depende de la asunción de un compromiso anterior. Como expone JUSTE RUIZ, en la Sentencia relativa al asunto Barcelona Traction, antes mencionada, "*el Tribunal ha afimado inequívocamente la legitimación sustancial de todos los Estados para*

---

152 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p. 559.

153 *Ibidem*; p. 599. En concreto, la Norma 149 enumera las siguientes:

"*a) las violaciones cometidas por sus órganos, incluidas sus fuerzas armadas;*

b) las violaciones cometidas por personas o entidades autorizadas a ejercer prerrogativas de su autoridad gubernativa;

c) las violaciones cometidas por personas o grupos que actúan de hecho obedeciendo sus instrucciones o bajo su dirección o control; y

d) las violaciones cometidas por personas o grupos privados que él reconoce y acepta como comportamiento propio".

exigir el cumplimiento de las obligaciones erga omnes[154]". Así ha quedado, también, establecido también en la Norma 140 de la misma Compilación, que afirma que «*La obligación de respetar y hacer respetar el derecho internacional humanitario no depende de la reciprocidad*»[155], pues el repetido artículo 1 común a los Convenios de Ginebra, impone dicha obligación, "*en todas las circunstancias*".

Esta costumbre internacional, recogida en la citada Compilación, ha sido, asimismo, reconocida por la Jurisprudencia internacional. Así, la CIJ, en su Opinión Consultiva, emitida en relación a las consecuencias de la presencia continuada de Sudáfrica en Namibia, expresamente declaró que la misma resultaba contraria a la legalidad internacional de tal modo que ningún Estado que tuviera relaciones jurídicas con Sudáfrica, en relación a Namibia, pudiera esperar la validez de las mismas. Es decir, en palabras de la CIJ,

> "In the view of the Court, the termination of the Mandate and the declaration of the illegality of South Africa's presence in Namibia are opposable to all States in the sense of barring erga omnes the legality of a situation which is maintained in violation of international law: in particular, no State which enters into relations with South Africa concerning Namibia may expect the United Nations or its Members to recognize the validity or effects of such relationship, or of the consequences thereof. The Mandate having been terminated by decision of the international organization in which the supervisory authority over its administration was vested, and South Africa's continued presence in Namibia having been declared illegal, it is for non-member States to act in accordance with those decisions[156]".

Y, más recientemente, Tribunal Penal Internacional para la antigua Yugoslavia (en adelante, TPAY), en la sentencia dictada en el asunto *Kupreskic,* en el año 2000, declaró expresamente que las obligaciones jurídicas de carácter

154 JUSTE RUIZ, J., *Las obligaciones erga omnes en Derecho Internacional Público*, en Estudios de Derecho Internacional, Homenaje al Profesor Miaja de la Muela, T.I, Madrid, pp. 219 a 233, en particular, p. 229.
155 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p. 563.
156 Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, I.C.J. Reports 1971; par. 126.

humanitario no podían depender de la reciprocidad[157]. En el citado fallo, el Tribunal no deja resquicio a la duda en cuanto a la inviabilidad de tal requerimiento y, por lo tanto, de la reciprocidad de las normas de DIH. Esta afirmación se ve reforzada, a juicio del Tribunal, en la ausencia de práctica al respecto y así establece que, "*there is in fact no support either in State practice or in the opinions of publicists for the validity of such a defence*[158]". Así, el TPAY dejó claramente establecido que, en ningún modo, puede aceptarse que el DIH esté basado en tal intercambio de derechos y obligaciones.[159]

Este punto es donde el TPAY hace una referencia expresa a la responsabilidad internacional del Estado, por omisión, cuando entiende que el efecto *erga omnes* de las normas de DIH genera responsabilidad internacional del Estado, tanto por acción como por omisión. En este sentido, el Tribunal entiende que dicha responsabilidad "(…) *for serious violations of international humanitarian law may not be thwarted by recourse to arguments such as reciprocity*." Esta postura se justifica en que las normas de DIH no protegen los intereses del Estado, sino que

---

157 "*Defence counsel have indirectly or implicitly relied upon the tu quoque principle, i.e. the argument whereby the fact that the adversary has also committed similar crimes offers a valid defence to the individuals accused. This is an argument resting on the allegedly reciprocal nature of obligations created by the humanitarian law of armed conflict. This argument may amount to saying that breaches of international humanitarian law, being committed by the enemy, justify similar breaches by a belligerent. Or it may amount to saying that such breaches, having been perpetrated by the adversary, legitimise similar breaches by a belligerent in response to, or in retaliation for, such violations by the enemy. Clearly, this second approach to a large extent coincides with the doctrine of reprisals, and is accordingly assessed below. Here the Trial Chamber will confine itself to briefly discussing the first meaning of the principle at issue*". ITYC PROSECUTOR v. Zoran KUPRE[KI], Mirjan KUPRE[KI], Vlatko KUPRE[KI], Drago JOSIPOVI], Dragan PAPI], Vladimir [ANTI], also known as "VLADO", IT-95-16-T, 14 January 2000; par. 515.

158 En este fallo, el TPAY trata lo que el mismo denomina, "*The Tu Quoque Principle is Fallacious and Inapplicable: The Absolute Character of Obligations Imposed by Fundamental Rules of International Humanitarian Law*", a lo largo de los párrafos 515 a 520. En concreto, la afirmación que aquí se recoge, es formulada en el párrafo 516. ITYC PROSECUTOR v. Zoran KUPRE[KI], Mirjan KUPRE[KI], Vlatko KUPRE[KI], Drago JOSIPOVI], Dragan PAPI], Vladimir [ANTI], also known as "VLADO", IT-95-16-T, 14 January 2000.

159 Al contrario, a juicio del Tribunal: "(…) *the bulk of this body of law lays down absolute obligations, namely obligations that are unconditional or in other words not based on reciprocity. This concept is already encapsulated in Common Article 1 of the 1949 Geneva Conventions, which provides that «The High Contracting Parties undertake to respect [...] the present Convention* in all circumstances» *(emphasis added). Furthermore, attention must be drawn to a common provision (respectively Articles 51, 52, 131 and 148) which provides that «No High Contracting party shall be allowed to absolve itself or any other High Contracting Party of any liability incurred by itself or by another High Contracting Party in respect of breaches referred to in the preceding Article [i.e. grave breaches]. Ibidem;* par. 517.

"*they were primarily designed to benefit individuals qua human beings*[160]". Es decir, que estas normas no pueden ser equiparadas a otras de naturaleza igualmente internacional, pero de contenido, por ejemplo, comercial, que si pretenden la protección de tales intereses.

A la vista de la interpretación contenida en el fallo que se examina, puede concluirse que, obviar los efectos *erga omnes* de la aplicación de las normas de DIH sería tanto como privarlas de su carácter humanitario. Como consecuencia de lo anterior, el Tribunal entiende, además, que las normas de DIH establecen obligaciones a la Comunidad Internacional en su conjunto y, en consecuencia, el interés jurídico en su cumplimiento, así como en su posible exigencia, corresponde a todos y cada uno de los Estados miembros de esa Comunidad[161], tal y como se verá con mayor profundidad en el Capitulo cuarto.

Pues bien, como afirma el comentario a la Norma 140 de la Compilación de DIH consuetudinario, "*este principio es válido para cualquier obligación de carácter humanitario, ya sea en los conflictos armados internacionales o en los no internacionales*" [162].

En este punto, el planteamiento del conflicto armado, tal y como hasta ahora era conocido, también exige una revisión de determinados conceptos que serán abordados en profundidad, en el Capítulo posterior. En cualquier caso, es preciso, ahora, exponer que podemos encontrarnos con ataques cibernéticos que se desarrollen en el ámbito de una ciberguerra, es decir, aquéllos en los que el elemento cibernético resulte el único que sea empleado en el curso de un

160 El TPAY realiza, en este caso, una puntualización, relativa a la responsabilidad, derivada del incumplimiento grave de las obligaciones de DIH que podrían considerarse imperativas sobre las que se volverá mas adelante, al tratar las normas de ius cogens. *Ibidem;* par. 517 a 520.

161 ICTY, *Kupreskic case*, Judgement, 14 January 2000; par. 515–518. La cita aparece, asimismo, recogida en la Compilación de DIH Consuetudinario. HENCKAERTS, J.M and DOSWALD-BECK, L. Customary International Humanitarian Law. Volume II Practice. Part 2. Cambridge University Press. 2005; pp. 3194 -3195. El Tribunal, literalmente estableció: "(…) *lay down obligations towards the international community as a whole, with the consequence that each and every member of the international community has a "legal interest" in their observance and consequently a legal entitlement to demand respect for such obligations". Furthermore, most norms of international humanitarian law, in particular those prohibiting war crimes, crimes against humanity and genocide, are also peremptory norms of international law or jus cogens, i.e. of a non-derogable and overriding character*"; p.519 *in fine*.

162 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p. 564.

conflicto armado, o con ciberoperaciones, que serán aquéllas que, utilizando internet, sean empleadas, en concurso con otros métodos de combate convencionales. Por último, hay que incluir, en esta primigenia clasificación, aquellos ciberataques potenciadores de un conflicto armado. Pues bien, éstos pueden ser dirigidos hacia cualquier objetivo que resulte especialmente sensible para la Defensa Nacional de un Estado y, por ello, resulta preciso abordar hasta qué punto o en qué ámbito el Estado es responsable de evitar que ello ocurra, pues son muchos los objetivos militares y civiles, susceptibles de ser combatidos a través de ciberataques y, sin duda, la protección frente a los mismos es uno de los mayores retos de los Estados modernos.

En este sentido, también resulta ilustrativa, la sentencia en el asunto *Eichmann,* en 1961, dictada por el Tribunal de Distrito de Jerusalén (Israel), en cuyo fallo se atribuyó los actos ilícitos cometidos por el acusado, a Alemania al ser considerados los mismos como "*actos del Estado*"[163].

Por otra parte, el Proyecto, además, añade que: "*El Estado que presta ayuda o asistencia a otro Estado en la comisión por este último de un hecho internacionalmente ilícito es responsable internacionalmente por prestar esa ayuda o asistencia*[164]". Pues bien, dicha previsión ha de tenerse especialmente en cuenta en el contexto en que, actualmente, se desarrollan los conflictos bélicos, pues será previsible que las

163 Sin perjuicio de volver sobre ello, el momento de examinar las cuestiones relativas a la atribución del hecho ilícito, es necesario tener presente, en este momento los fundamentos expresados por el citado Tribunal: "(…) *Further on, the judgment draws a distinction between the substantive principles of international law which lay down that "war crimes" and "crimes against humanity" are crimes whenever and wherever they were committed, and the actual enforcement of these universal principles which may come up against barriers of national sovereignty: "We are empowered to determine the guilt or innocence of persons accused of acts described as "war crimes" and "crimes against humanity" under rules of international law. At this point, in connection with cherished doctrines of national sovereignty, it is important to distinguish between the rules of common international law which are of universal and superior authority on the one hand, and the provisions for enforcement of those rules which are by no means universal on the other... As to the punishment of persons guilty of violating the laws and customs of war (war crimes in the narrow sense), it has always been recognized that tribunals may be established and punishment imposed by the state into whose hands the perpetrators fall. (...) Applying these principles, it appears that the power to punish violators of international law in Germany is not solely dependent on the enactment of rules of substantive penal law applicable only in Germany (...) The judgment proceeds to say (p. 983): "Whether the crime against humanity is the product of statute or of common international law, or, as we believe, of both, we find no injustice to persons tried for such crimes. They are chargeable with knowledge that such acts were wrong and were punishable when committed."* Asunto *Eichmann,* en 1961. A-G Israel v. Eichmann (1968), 36 ILR 5 (Tribunal de Distrito de Jerusalén); par. 26.

164 Articulo 16 del Proyecto de artículos.

Fuerzas Armadas de un Estado actúen en apoyo de las de otro Estado aliado. Asimismo, puede darse el supuesto de que éstas actúen junto con otras, formando parte de una coalición internacional, sin necesidad de estar sujetas al mandato de una Organización Internacional. En esos casos, la ayuda o asistencia prestada tendrá la misma consideración que la violación de una obligación internacional respecto del Estado que presta ayuda o asistencia.

5.1. La conducta omisiva de un Estado que puede desencadenar un ciberataque armado, frente a otro Estado.

La comisión por omisión de un hecho ilícito internacional no plantea dudas y, desde el punto de vista de la exigencia de responsabilidad internacional al Estado, resulta irrelevante que el incumplimiento de la obligación internacional se realice a través de una conducta activa u omisiva. Así se concluye del examen de la legalidad internacional, convencional y consuetudinaria, pudiendo afirmarse, además, que esta perspectiva ha sido admitida, desde hace décadas, por la jurisprudencia internacional.

Por lo tanto, el siguiente paso a dar en este análisis consistirá en indagar cuáles pueden ser las consecuencias de dicha omisión. Es decir, en el contexto que aquí se aborda, habrá que estudiar si dicha omisión puede conllevar el incumplimiento de las normas de DIH en el lanzamiento de un ciberataque y en qué supuestos puede tener lugar dicho ataque.

Para ello hay que hacer alusión a dos situaciones que, con carácter principal, pudieran darse en el ámbito de los ciberataques, de igual modo que se producen en el desarrollo de conflictos, en los que se emplean métodos de combate tradicionales.

En primer lugar, habrá que hacer referencia a los actos cometidos por beligerantes que no pertenecen a las Fuerzas Armadas de un Estado y, por lo tanto, actúan al margen de cualquier control estatal. Por otra parte, también será necesario analizar en qué tipo de responsabilidad por omisión incurre el Estado que no impide la comisión de un ciberataque por parte de quienes pertenecen a sus Fuerzas Armadas, así como la responsabilidad de quienes, perteneciendo a

dichas Fuerzas Armadas, no impiden que el ataque cibernético sea perpetrado por un subordinado.

5.1.1. La aplicabilidad de la doctrina contra insurgencia a los ataques cibernéticos lanzados fuera del control del Estado.

Como los recientes acontecimientos relativos a los ciberataques, han puesto de manifiesto, es evidente que, en el uso de este medio cibernético habrá que tener en cuenta la posible presencia de personas que, sin contar con la consideración de agentes del Estado, actúen de forma contraria a las normas de DIH. De forma cada vez más habitual se constata, incluso, la presencia de personas que se hallan fuera del control de los órganos del Estado en cuestión. La presencia física de insurgentes, terroristas u otro tipo de activistas, en el desarrollo de los conflictos armados internacionales y no internacionales, resulta incuestionable y consustancial a la nueva tipología de los conflictos armados. En el caso de los ciberataques, todavía resulta más decisiva dicha presencia, pues el "armamento" se halla en manos de millones de individuos que pueden entrar a formar parte de los combatientes en cualquier momento.

No se trata aquí tanto de delimitar cuestiones, que serán objeto de estudio al abordar la atribución del hecho ilícito, en el Capítulo tercero, como de sentar las bases, desde un punto de vista práctico, abordando la posibilidad de cometer el hecho por omisión para, posteriormente, tenerlas en cuenta, precisamente, al tratar de la atribución.

De acuerdo con la doctrina publicada por la OTAN, las actividades de insurgencia son aquéllas que provienen de un grupo o movimiento, normalmente organizado. Sin embargo, en la lucha contra las mismas, no pueden ser ignorados "*the destabilising effects of irregular activity*". Esta actividad irregular, por su parte, constituye "*the use or threat of force by irregular forces, groups or individuals, frequently ideologically or criminally motivated, to effect or prevent change*

as a challenge to governance and authority[165]". La preocupación de la Alianza por este tipo de actividades y la lucha contra ellas nace, precisamente, de la amenaza que supone la omisión por parte de las autoridades internas del Estado, de las medidas tendentes al control de dichas actuaciones de insurgencia[166]. En este sentido, pueden asumirse los presupuestos que definen la asimetría del conflicto, cuando la misma se deriva de la realización de actuaciones terroristas. Es decir, los mismos condicionantes que pueden encontrase en ese tipo de conflictos, podrían aplicarse a los ataques informáticos llevados a cabo por individuos que se posicionen al margen de la actuación de un Estado. Así, por ejemplo, del terrorismo, como factor asimétrico del conflicto, se ha dicho que "*Sus nuevas formas no enfatizan la búsqueda de una paridad de fuerzas, sino que el empleo de tácticas y medios no convencionales son estrategias de negación y propaganda. Su dinámica se sitúa así entre el pasquín y la bomba, con una tendencia a utilizar los medios civiles (por ejemplo, los medios de transporte) como originales armas de guerra*[167]". No parece pues, que estas apreciaciones resulten completamente ajenas al factor cibernético, que pueda estar presente en los conflictos armados.

Será en este contexto, pues, en el que puedan producirse determinados ataques cibernéticos, como consecuencia de la ausencia de control interno, por parte del Estado desde el que se ejecutan, bien por una deliberada falta de interés en ello, bien por una imposibilidad material de prestar esa seguridad interna.

La realización de estas actuaciones, al margen del Estado, conlleva, de forma habitual, la violación de las normas de DIH aplicables al combate pues, como afirma GEISS, "*A causa de la evidente disparidad de la capacidad militar de los*

---

165 El documento de OTAN AJP-3.4.4 - ALLIED JOINT DOCTRINE FOR COUNTERINSURGENCY, publicado en febrero de 2011, define las actividades de insurgencia como: "*the actions of an organised, often ideologically motivated, group or movement that seeks to effect or prevent political change of a governing authority within a region, focused on persuading or coercing the population through the use of violence and subversion*". AJP-3.4.4 - ALLIED JOINT DOCTRINE FOR COUNTERINSURGENCY; p.1-2, par.0109.

166 Documento de OTAN AJP-3.4.4 - ALLIED JOINT, doc. cit.; pp.1-2 y 1-3, par.0111 y 0112.

167 De este modo se manifiesta AZNAR, al tratar de los conflictos asimétricos y la participación de terroristas en los mismos. AZNAR FERNADEZ DE MONTESINOS, F. *Terrorismo y estrategia asimétrica*. Documento de Opinión 9/2011. Enero de 2011. Instituto Español de Estudios Estratégicos; p.3. Disponible en:http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO09_2011TerrorismoEstrategiaAsimetrica.pdf.Fecha de consulta, marzo de 2013.

beligerantes en algunos conflictos contemporáneos, los incentivos para violar el DIH parecen haber alcanzado comparativamente nuevas cotas[168]". De este modo, en los actuales conflictos, de corte asimétrico, la violación de las normas de DIH no puede considerarse excepcional, sino, antes bien, como pone de manifiesto el mismo autor, "*se ha convertido en un rasgo estructural recurrente que caracteriza, desde el principio, a muchos de los conflictos armados actuales*[169]".

En adición a lo anterior, habrá que tener presente que el dominio por los llamados "*global commons*" o espacios globales es una de las cuestiones estratégicas de mayor actualidad. Como pone de manifiesto KUTT "*cualquier enfrentamiento que se produzca en un futuro deberá desarrollarse necesariamente y de manera primordial en el ámbito de los espacios comunes, dado que es precisamente en el dominio de estos espacios donde residen los fundamentos de la hegemonía internacional*[170]". En este sentido, el mismo autor justifica dicha afirmación en el informe publicado por la OTAN, en relación al "*Acceso a los espacios comunes*", en el que la Organización afirma:

> "Adversaries will take the initiative and exploit Alliance vulnerabilities in both the virtual and physical domains of the global commons, including the realms of sea, air, space, and cyberspace. (…) Access to, and "unfettered use" of the commons must be ensured. (…) Access in particular is seen as "pivotal to the success of all Alliance operations[171]".

Por lo expuesto, en el contexto aquí descrito, se presenta la compleja cuestión de determinar en qué medida el Estado es responsable de la actuación de determinados individuos cuando, en realidad, no forman parte de las Fuerzas Armadas del Estado, ni actúan en nombre del mismo. Sin embargo, pudiera darse el caso de que su actuación se desarrollara en apoyo explícito y efectivo de

168 GEISS, R. *Las estructuras de los conflictos asimétricos.*, op cit.; p.5.
169 GEISS, R., *Las estructuras de los conflictos asimétricos*, op.cit.; p.5.
170 KUTT NEBRERA, A., *La importancia de dominar los global commons en el siglo XXI*. Instituto Español de Estudios Estratégicos. Documento Marco 29/2012, de 12 de Noviembre de 2015; p.4. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf. Fecha de consulta, enero 2016.
171 El informe de OTAN, aquí recogido, es citado por KUTT NEBRERA, A. *La importancia de dominar los global commons en el siglo XXI*,op.cit.; p. 5.

los intereses de una de las Partes en conflicto. En el supuesto de que dichos beligerantes actuaran contraviniendo el DIH, en un conflicto armado internacional o no internacional, podríamos encontrarnos ante la imposibilidad de que el Estado al que pertenecen resultara responsable de su actuación, de forma directa. Como se ha adelantado, ésta es una cuestión relativa, principalmente, a las cuestiones de atribución de la conducta y, por lo tanto, será objeto de examen más detallado en el Capítulo correspondiente. Sin embargo, resulta imprescindible abordarlo en relación a las cuestiones que pueden suscitarse al determinar la responsabilidad internacional del Estado por omisión.

En este punto hay que plantear qué tipo de responsabilidad es exigible a un Estado que no impide que sus nacionales reciban ciberberataques, lanzados por beligerantes respecto de los que no ejerce ningún tipo de control. En principio, nada impediría la exigencia de dicha responsabilidad siempre y cuando el Estado estuviera en condiciones de prestarla. Es decir, será preciso aquí tener en cuenta que el nivel de desarrollo tecnológico de los Estados resultará un elemento a valorar a la hora de concluir si las medidas de seguridad tomadas en el ciberespacio son o no suficientes.

En el caso de España, dichas medidas vienen genéricamente planteadas en la citada Estrategia de Seguridad Nacional de 2013 (en adelante, ESN)[172] y también en la Estrategia Nacional de Ciberseguridad (en adelante, ENC)[173]. Ambos documentos identifican los riesgos y amenazas que pueden cernirse sobre el ciberespacio y pueden afectar a España. A través de la ENC, el Gobierno de España se propone el objetivo de "*Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia*", así como de "*Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular*[174]".

172 Estrategia de Seguridad Nacional. Un Proyecto Compartido, Presidencia del Gobierno, 2013.
173 La Estrategia de Ciberseguridad Nacional fue aprobada el pasado 5 de diciembre de 2013 por el Consejo de Seguridad Nacional.
174 Estrategia de Ciberseguridad Nacional; doc. cit.; pp. 21-23.

Pues bien, en la protección de dichas infraestructuras, desde el punto de vista jurídico, habrá que tener en cuenta lo establecido en la Ley 8/2011 de Protección de las Infraestructuras Críticas y su reglamento de desarrollo, toda vez que ambas normas establecen un sistema de protección de las mismas, tendente a conseguir los objetivos propuestos por el Gobierno, en los precitados documentos. Ello quiere decir que, en España, se cuenta con un acervo normativo que obliga al Estado, y al resto de los agentes involucrados, sean públicos o privados, a dotarse de una seguridad. Este concepto de seguridad engloba, indudablemente, el aspecto cibernético de las infraestructuras, que prestan soporte a los servicios que se consideran esenciales para el normal desenvolvimiento de la vida en sociedad y que aparecen recogidos en doce sectores estratégicos, incluidos en el Anexo de la citada Ley. Habida cuenta la amplitud de dichos sectores y la naturaleza de los mismos, parece sencillo imaginar un ciberataque que, llevado a cabo por insurgentes contraviniendo el DIH, pudiera poner en peligro la seguridad de los nacionales, dirigiéndose, precisamente, contra alguno de los doce sectores estratégicos[175].

La exigencia de este tipo de responsabilidad, basada en la omisión de las medidas de seguridad que el Estado está obligado a ofrecer, tampoco resulta una cuestión novedosa. Antes bien, ya en este sentido se expresó el Tribunal Internacional responsable de conocer del asunto del personal diplomático y consular de los Estados Unidos en la Embajada de Teherán. Este Tribunal entendió que el Estado de Irán no podía ser responsable, de forma directa, por los hechos acaecidos en la sede diplomática de los Estados Unidos. Sin embargo, sí que encontró responsable al mismo por omitir la adopción de las necesarias medidas de protección de dicha sede en su territorio[176].

---

175 Los sectores estratégicos citados en el Anexo de la Ley 8/2011 son los siguientes: Administración, Alimentación, Energía, Espacio, Sistema Financiero y Tributario (por ejemplo, banca, valores e inversiones), Agua (embalses, almacenamiento, tratamiento y redes), Industria Nuclear, Industria Química, Instalaciones de Investigación, Salud, Tecnologías de la Información y las Comunicaciones y Transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico). Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. BOE núm. 102, de 29 de abril de 2011.

176 Así se expresó el Tribunal al respecto: "*The conclusion just reached by the Court, that the initiation of the attack on the United States Embassy on 4 November 1979, and of the attacks on the Consulates at*

En el estudio que aquí se plantea, sin embargo, la cuestión de ofrecer el nivel óptimo de seguridad (ciberesiliencia), no queda, únicamente, residenciado en el Estado. Antes bien, otras Administraciones Públicas, e incluso agentes privados que pudieran ser gestores de redes, utilizadas para la prestación de dichos servicios esenciales, han sido involucrados por la citada Ley 8/2011, en la provisión de esa seguridad cibernética.

En el supuesto, pues de que un individuo o grupo de individuos, atacara una red cibernética, de tal modo que se impidiera el acceso de los ciudadanos a servicios tales como la banca privada o la electricidad, sería preciso determinar el nivel de responsabilidad realmente atribuible al Estado. Durante el desarrollo de un conflicto armado internacional o no internacional, no resultaría improbable que ese individuo o grupo de individuos dirigiera un ciberataque a alguna de las infraestructuras críticas, responsables de gestionar servicios como el suministro de agua, transporte o red electrica. La asimetría que se observa en el desarrollo de los conflictos actuales, conduce a pensar, precisamente, que ésta sería una incidencia de probable comisión. En ese caso, habría que cuestionarse en qué medida el Estado pudiera ser responsable por la omisión de las medidas de seguridad ofrecidas a los ciudadanos en materia cibernética.

Sin embargo, por más que el responsable último de nuestra seguridad sea el Estado, no puede ello confundirse con una asunción de la totalidad de las funciones relativas a este asunto. Antes bien, resulta crucial, en este punto, la concienciación de todos los agentes, incluidos los privados, en la realización de las tareas tendentes a lograr dicha seguridad cibernética. Todo ello, sin perjuicio de que, como se ha dicho, las obligaciones de cada uno de los agentes, concernidos en este ámbito, quedan reflejadas en la normativa citada, de manera que el incumplimiento de estas obligaciones por quienes están obligados a ello, podría llegar a originar dicha responsabilidad. No obstante, el papel que juegan

---

Tabriz and Shiraz the following day, cannot be considered as in itself imputable to the Iranian State does not mean that Iran is, in consequence, free of any responsibility in regard to those attacks; for its own conduct was in conflict with its international obligations. By a number of provisions of the Vienna Conventions of 1961 and 1963, Iran was placed under the most categorical obligations, as a receiving State, to take appropriate steps to ensure the protection of the United States Embassy and Consulates, their staffs, their archives, their means of communication and the freedom of movement of the members of their staff". United States Diplomatic and Consular Staff in Tehran, Judgment, I. C. J. Reports 1980; par. 61.

los responsables de estas infraestructuras, requiere un estudio más profundo y, por ello, será abordado de modo más completo, en el Capítulo concerniente a la atribución del hecho ilícito.

5.1.2.- Responsabilidad por omisión de los miembros de las Fuerzas Armadas.

Si bien es probable la participación de agentes no estatales en el conflicto, la cuestión de la actuación de quienes se hallan, directamente, implicados en el mismo, es evidente. Por este motivo, se trata aquí de aproximarse al estudio de dicha actuación por omisión para, como en el caso anterior, señalar los supuestos que, con posterioridad, serán abordados en relación con la posible atribución de su conducta al Estado.

Una vez más, el cumplimiento de las normas de DIH, en el uso de internet como método de combate, resulta insoslayable. Sin embargo, dicho cumplimiento requiere, indefectiblemente, un conocimiento preciso tanto del método de combate como de las normas de DIH que, a su vez, permita tener conciencia del alcance y contenido de dichas normas, al objeto de no incurrir en su incumplimiento, también por omisión. Se habla aquí de conocimiento preciso, por cuanto, como se viene exponiendo, las posibilidades de uso de este método de combate exigen una interpretación del DIH que resulte aplicable a los conflictos armados.

Por lo tanto, esta necesidad de conocer no puede ser planteada únicamente desde el punto de vista global que exige el DIH, sino que tendrá que venir referida, además, a la especificidad del elemento cibernético. Por otra parte, el conocimiento del DIH no puede ser contemplado como un objetivo deseable, sino que alcanza el rango de norma de obligado cumplimiento, desde el momento en que, la obligación de conocer se halla recogida en la Compilación de DIH Consuetudinario. De este modo, la Norma 142 de dicha Compilación impone a los Estados y las partes en conflicto la obligación de impartir "*cursos de formación*

en derecho internacional humanitario a sus fuerzas armadas"[177]. En el supuesto de los ciberataques, esta obligación cobra una especial relevancia.

No puede aquí olvidarse la reflexión, previamente expuesta, en relación a la doble vertiente de uso que permite este elemento, así como a su gran utilidad para las Fuerzas Armadas durante el desarrollo del conflicto. Es decir que, a diferencia de otras armas, ésta que nos ocupa será empleada de forma lícita y pacífica, en la gran mayoría de las ocasiones. Pero, además, es preciso tener en cuenta que se trata de un arma que permite una accesibilidad especialmente sencilla y un manejo, igualmente asequible, por gran parte de la población. Es decir, de igual modo que no es previsible que un arma nuclear, por ejemplo, se encuentre al alcance de todos los componentes de un Contingente que se halle desempeñando una Operación de Mantenimiento de la Paz, sí que es completamente asumible que todos ellos cuenten con un smartphone para uso particular. El uso que de ese "arma" pudiera llegar a hacerse, dependerá en gran medida del nivel de formación de los componentes del Contingente.

Por lo tanto, el deber de impartir cursos de formación en DIH, que la citada Compilación impone a los Estados, se presenta, en este ámbito, revestida de una serie de especificidades que hay que contemplar. Nuevamente, deberá interpretarse esta obligación[178], a la luz del empleo de las armas basadas en las nuevas tecnologías.

Así, podrán distinguirse dos aspectos a tener en cuenta en este supuesto: la obligación del Estado de formar a los componentes de sus Fuerzas Armadas sobre el contenido del DIH, realizando una especial previsión sobre la interpretación del mismo en las ciberoperaciones. Y, por otro lado, la obligación de éstos, de formar a sus subordinados, advirtiéndoles de que el uso indebido de internet podría conllevar el lanzamiento de un ataque armado.

177 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p.566.

178 Esta obligación tiene una larga tradición en el DIH convencional, de modo que ya se hallaba contemplada en los Convenios de Ginebra de 1906 y 1929.37 Posteriormente, se reafirmó en los Convenios de Ginebra de 1949 y sus Protocolos adicionales, en la Convención de La Haya para la protección de los bienes culturales y su Segundo Protocolo, y en la Convención sobre ciertas armas convencionales, como se pone de manifiesto en HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p.566.

Pues bien, en relación al primero de los aspectos apuntados, será crucial que se imparta la adecuada formación en DIH por cuanto, en el contexto bélico en el que se suceden este tipo de acciones, los comportamientos realizados por los subordinados, pudieran dar lugar a la exigencia de responsabilidad respecto de sus superiores jerárquicos. En aquéllos casos en que éstos conozcan o tengan información que les permita concluir que el subordinado estaba cometiendo o iba a cometer tal infracción, será exigible dicha responsabilidad, en tanto que la ignorancia no puede eximir del cumplimiento del DIH, por más que sea una de las principales causas de su inobservancia[179].

Antes bien, el deber de supervisión, por parte de los Mandos, respecto de las actuaciones de quienes se encuentren a sus órdenes, obliga a tener aún más en cuenta dicho deber. Asimismo, la obligación que aquéllos tienen, de actuar en el ámbito que les ha sido dado, es decir el disciplinario o penal, conduce a la misma conclusión. La previsión en DIH de esta obligación vuelve a encontrarse en la Compilación de DIH Consuetudinario, cuando en su Norma 144 establece que "*Los Estados no alentarán las violaciones del derecho internacional humanitario por las partes en un conflicto armado. En la medida de lo posible, deberán ejercer su influencia para hacer que cesen esas violaciones*".[180]

Como ya se ha puesto de manifiesto, el artículo 1 común a los Convenios de Ginebra establece la obligación de "*hacer respetar*", de tal forma que el conocimiento de las normas de DIH se presenta como un deber. El CICR entiende esta obligación, en "*la idea de que un factor esencial para su aplicación efectiva y, por consiguiente, para la protección de las víctimas de los conflictos armados, es tener un buen conocimiento de sus normas*". Asimismo, el Comité, al respecto considera esta obligación de difusión, como el "*corolario del compromiso de los Estados Partes en los*

179 Así lo entiende asimismo BOLLO AROCENA quien, además, recuerda que una de las obligaciones de todos los Estados parte en los Convenios de Ginebra consiste en formar al personal civil y militar que tenga la responsabilidad de aplicarlo. BOLLO AROCENA, M. D., *La responsabilidad internacional del Estado por la violación del Derecho Internacional Humanitari*o, op.cit.; p.159.

180 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p.575.

instrumentos de DIH de respetar y hacer respetar las disposiciones que éstos contienen[181]".

Esta interpretación del artículo 1 común, que implica obligaciones, más allá de las de las partes en conflicto, ha recibido un constate apoyo por parte de las Organizaciones Internacionales. En numerosas ocasiones ha sido el Consejo de Seguridad de las Naciones Unidas[182]; sin embargo, por el contexto que aquí se analiza, resulta más representativa la realizada por el Comité de Asuntos Civiles de la OTAN que en Informe de septiembre de 1999, estableció que

> "Principles such as the prohibition of torture or attacks on the physical and moral integrity of persons which are at the heart of all these texts are regarded by lawyers as entailing erga omnes obligations, i.e. obligations that states must respect in all circumstances without any contractual exception or requirement of reciprocity[183]".

La obligación pues, de respetar el DIH, durante el desarrollo del conflicto armado, pasará por ofrecer a los Mandos de las Fuerzas Armadas en combate, la formación necesaria al respecto, haciendo constar expresamente que, como se viene poniendo de manifiesto, el lanzamiento de ciberataques, en modo alguno puede quedar exento de dicho cumplimiento. Antes bien, se advierte aquí, la necesidad de proveer de un adiestramiento lo suficientemente eficaz como para no incurrir en errores en el normal desarrollo de las operaciones. Es decir, la equiparación del ciberataque al ataque armado deberá ponerse de manifiesto, en los términos que han sido expuestos, así como las limitaciones en el lanzamiento de dichos ciberataques que, han sido anticipadas y se abordarán en el Capítulo próximo, por constituir el contenido de la obligación internacional a la que aquí

181 Ambas consideraciones son realizadas en el Documento de Cruz Roja, CICR, Servicio de Asesoramiento en Derecho Internacional Humanitario, *La obligación de difundir el derecho internacional humanitario*. Febrero de 2003; p. 1. Documento disponible en el sitio web: https://www.icrc.org/spa/assets/files/other/obligacion_difundir_dih.pdf. Fecha de consulta, marzo de 2013.

182 Estas Resoluciones aparecen recogidas en HENCKAERTS, J.M. y DOSWALD-BECK, vol.II, op.cit.; pp. 3168-3173.

183 NATO Civilian Affairs Committee. *Kosovo as a precedent: towards a reform of the Security Council?* International Law and humanitarian intervention. Arthur Paecht. General Rapporteur. 16 de septiembre 1999; par. 29.

se hace referencia. Esta formación en DIH, imperativa, en cualquier caso, debe pasar por una específica atención a quienes, en el desarrollo del conflicto, tengan encomendada la labor de selección de objetivos, o *targeting*, así como a quienes se encuentren especialmente encargados de las operaciones cibernéticas, de modo que, en su ejecución, se tengan presentes los principios de DIH, aplicables al combate, sin perjuicio del método de combate que sea utilizado en cada caso, en los términos expresados por la CIJ.

Esta equiparación, en relación a la exigencia de cumplimiento del DIH que, tradicionalmente, ha realizado la Jurisprudencia Internacional, con independencia del método de combate que sea utilizado, se ve reforzada por la previsión penal antes apuntada. Es decir, que, precisamente, al personal que aquí se cita, le resulta de aplicación, el CPM, tanto en tiempo de guerra como de paz. De conformidad con dicho Código, la utilización de un arma convencional o cibernética resulta indiferente a la hora de dirimir la responsabilidad penal, pues la prestación de un servicio de armas incluye ambas opciones.

En primer lugar, procedería una específica formación, aunque sea de modo genérico, al resto de los componentes de las Fuerzas Armadas. En efecto, pudiera ocurrir que muchos de ellos, pese a encontrarse en el Teatro de Operaciones, no se hallen en posición de entrar en combate o lanzar un ciberataque. Sin embargo, lo más probable es que todos ellos dispongan de un dispositivo informático o telefónico, de uso propio, que permita su acceso a internet. Sería muy recomendable, en consecuencia, que sus Mandos advirtieran de la necesidad de conocer el alcance del uso de dichos dispositivos. Desde una visión realista, parece improbable que, a través de un terminal de uso particular, pudiera llegar a darse un ataque armado que supusiera la violación de una norma de DIH. Sin embargo, no puede ignorarse la posibilidad de participación en redes sociales o la utilización del mismo para la propagación de correo masivo u otras actuaciones que pudieran dar lugar a una actuación que otro Estado pudiera entender como un ciberataque. Es conveniente volver a recordar que todavía no existe un concepto de ciberataque que lo equipare al ataque armado en el Derecho Convencional internacional y, también, que la mayoría de los

ciberataques que hasta ahora han planteado dudas en cuanto a su calificación jurídica, no han provenido de un Estado ni de un contingente durante el desarrollo del combate. En una gran parte de los casos de los que se ha tenido constancia, han sido ataques provenientes, aparentemente, de personas civiles que, sin embargo, han presentado tal virulencia que han planteado a la Comunidad Internacional, dudas sobre su calificación jurídica. Por ello, un mal uso de internet, aun a título privado, podría originar una situación de, al menos, tensión con otro Estado, durante el combate, que debería evitarse a través de esa específica formación a todo el personal.

Cuestión distinta es la formación que debiera recibir el personal de las Fuerzas Armadas, a quien corresponde el planeamiento y desarrollo de Operaciones. En este sentido, sería imprescindible que la formación no abarcara, únicamente, los aspectos técnicos de los métodos a su alcance. En esta labor de formación y adiestramiento, resultaría más que conveniente poner de manifiesto que dicho método puede e incluso debe constituir un método de combate. Sin embargo, habrá de advertirse de la necesidad de que dicho método se adecue al imperativo cumplimiento de las normas de DIH, que ya ha sido reiteradamente expuesto.

En caso contrario, el desconocimiento de las normas podría conllevar que, por negligencia, resultara atacada una red informática destinada a usos civiles, ignorando así, la protección al no combatiente. También podría darse el supuesto de que, en ejecución de una ciberoperación, la otra parte en conflicto fuera objeto de engaño, aprovechando, precisamente, las posibilidades de anonimato y enmascaramiento que permite la red y que ello se realizara, de tal modo, que se violaran las normas relativas a la prohibición de perfidia.

Como tantas veces se ha puesto de manifiesto, internet será utilizado durante el conflicto armado, no sólo como método de combate, sino también, como mero medio de comunicación entre los componentes del Contingente en combate y entre el Mando de éstos y el Mando superior que pudiera hallarse fuera del Teatro de Operaciones, así como, entre quienes se encuentren en combate y sus Aliados. Pues bien, en la gestión de esas comunicaciones, también

deberá ponerse especial cuidado, tanto por parte de quienes las realizan como por parte de quienes están encargados de gestionar esos medios. En todo momento, el personal deberá hallarse suficientemente capacitado y también concienciado del alcance que puede llegar a tener un mal uso de internet. En este sentido, habrá que tener en cuenta que el mal uso puede deberse a una actuación intencionada, pero también, al error humano. Por lo tanto, aquéllos a quienes corresponda la gestión de los medios informáticos deberán reducir al máximo los riesgos que, por un uso incorrecto de internet, pudieran derivar en actuaciones, que podrían entenderse por la otra parte del conflicto, como un ciberataque.

Con independencia del origen y motivación de una actuación negligente, las consecuencias serían las mismas. En primer lugar, quedaría expuesta la vulnerabilidad del sistema y, en segundo lugar, podría originar una respuesta de la otra parte en el conflicto. Como se viene exponiendo, en el caso de los ciberataques, no nos encontramos ante una materia cuyo concepto y tratamiento jurídico hayan tenido una respuesta unánime. Al contrario, como ya ha quedado expuesto, algunos autores de la doctrina internacionalista abogan por un concepto bastante amplio de ciberataque como ataque armado. Ello conduce, inevitablemente, a la observancia de un especial cuidado y diligencia en la gestión de internet durante el conflicto. En caso contrario, podría darse la situación de que el contingente en combate que recibe un ciberataque respondiera, en todo caso, como si se tratara de un ataque armado, aun cuando el mismo no reuniera los requisitos que aquí se defienden, con base en una interpretación restrictiva. Por ello, en esta materia resulta crucial ofrecer una formación precisa, desde un punto de vista técnico, y adecuada, desde el ámbito de la aplicación del DIH a los conflictos armados, cuando en ellos se utilice el elemento cibernético.

Es, por lo tanto, tan previsible como indeseable que una deficiente formación en quienes se hallen encargados del desarrollo de las ciberoperaciones, diera lugar al lanzamiento de un ciberataque o ciberoperación, contrario a las normas de DIH. Ese incumplimiento no podría ser excusable, pues ya se ha puesto de manifiesto que al empleo de todo método de combate ha de aplicarse

el DIH. Tampoco podría escudarse, el Ejército en cuestión, en estar sufriendo ciberataques por parte de un combatiente que no respeta el DIH, pues también ha quedado establecido, a través de las decisiones jurisprudenciales traídas al estudio, que la reciprocidad en materia de DIH es inaplicable.

El hecho ilícito por omisión del Estado, en el uso de los ciberataques como método de combate podrá producirse cuando, por falta de formación específica o de medios adecuados, los componentes de sus Fuerzas Armadas transgredan las limitaciones impuestas en el combate.

El concepto de la responsabilidad por omisión, que aquí se invoca, fue establecido hace décadas en relación con los crímenes de guerra que, finalmente, se imputaron al General Yamashita[184]. Del examen de dicho fallo judicial, se desprende que, tras la II Guerra Mundial, la Corte Suprema de los Estados Unidos sostuvo que el mencionado General fracasó en el ejercicio del "control efectivo" sobre algunas de sus fuerzas subordinadas, de forma que éstas cometieron atrocidades que fueron consideradas crímenes de guerra. Entendió, asimismo, que el Derecho de la Guerra presupone que la violación del mismo ha de ser evitada, a través del control de las operaciones de guerra, por los Mandos. Éstos son, de alguna manera, por extensión, responsables de sus subordinados, de conformidad con lo dispuesto en el Anexo al Cuarto Convenio de La Haya de 1907; en el artículo 19 del Décimo Convenio; en el artículo 26 de la Convención de la Cruz Roja de Ginebra y, por último, en el artículo 44 del Anexo al Cuarto Convenio de La Haya[185].

En efecto, del incumplimiento de las normas de DIH, al margen de la responsabilidad individual que pudiera ser exigida y que no es objeto del presente estudio, se deriva, esencialmente, la responsabilidad del Estado infractor. Así se contempla, como ya se ha indicado, en la Norma 149 de la Compilación de DIH Consuetudinario.

184 Estas apreciaciones, se hallan contenidas en la Sentencia de la Corte Suprema de Estados Unidos, caso *Yamashita,* decisión de 4 de febrero de 1946.

185En cuanto a la específica responsabilidad del Mando militar, derivada de la conducción de ciberoperaciones, puede consultarse DE TOMÁS MORALES, S. y VELAZQUEZ ORTIZ, A.P. *La responsabilidad del mando en la conducción de operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz*, en Revista Española de Derecho Militar, núm.100. Ministerio de Defensa; enero–diciembre 2013; pp. 117-150.

6. CONCLUSIONES AL CAPÍTULO PRIMERO.

A lo largo del presente capítulo, destinado a examinar la comisión del hecho ilícito por acción y por omisión, se ha abordado, con carácter primordial, el concepto jurídico de ciberataque armado, como punto de partida para el examen del resto de las cuestiones relativas al régimen jurídico aplicable a los ciberataques cuando éstos se utilicen como método de combate. Del examen de estas cuestiones pueden extraerse las siguientes conclusiones.

PRIMERA: El concepto de ciberataque armado ha de basarse en criterios restrictivos. El concepto de ataque armado que hasta ahora ha sido manejado en el Derecho Internacional Convencional y Consuetudinario requiere una interpretación restrictiva, cuando se tratar de dirimir si un ciberataque, utilizado como método de combate, puede ser considerado un ataque armado.

El aparente vacío de legalidad que existe respecto de este método de combate y la ausencia de un concepto consolidado por parte de la doctrina internacionalista no pueden avalar un concepto de ciberataque que suponga una ampliación injustificada del concepto de ataque armado. Del examen de la prohibición del uso de la fuerza y la amenaza del uso de la fuerza contenidos en el artículo 2 de la Carta de Naciones Unidas, puede concluirse que los ciberataques constituyen una manifestación de ese uso de la fuerza. Esta conclusión se ve, además, reforzada por el concepto de crimen de agresión, presente en las Resoluciones 2625 y 3314 de la Asamblea General de Naciones Unidas. En definitiva, hay que concluir que los ciberataques pueden constituir un crimen de agresión, en los mismos términos que el resto de actos incluidos en este concepto.

Han de abandonarse, por lo tanto, las posturas de la doctrina internacionalista que abogan por un concepto amplio en el que pueden quedar incluidas actividades cibernéticas que no reúnen las condiciones que la legalidad internacional exige para calificar un hecho como ataque armado. La peculiaridad de este método de combate y las lagunas jurídicas que antes se apuntaban no pueden servir de justificación para adoptar un concepto de ciberataque armado

que sea contrario a la legalidad internacional. De ser así, se produciría una mayor indefinición conceptual, que, en absoluto, es deseable.

Por otra parte, si algo se ha puesto de manifiesto hasta ahora, ha sido la frecuencia y facilidad con que pueden producirse estos ataques cibernéticos. Asumir un concepto de ciberataque armado que permita incluir actividades de menor gravedad que las que conforman el concepto de ataque armado convencional, podría parecer, en principio, una solución viable, que diera respuesta a los ataques que se producen frecuentemente. Sin embargo, esa frecuencia de actividad ilícita en la red es la que justifica, precisamente, la delimitación restrictiva de los ataques cibernéticos. Estas otras actividades podrán encuadrarse, jurídicamente, en el ámbito penal interno o, en su caso, en la legalidad internacional aplicable al terrorismo.

Únicamente la adopción de un concepto restrictivo permitirá que la prohibición del uso y la amenaza de la fuerza sigan teniendo la vigencia necesaria y no queden desvirtuados. En consecuencia, hay que favorecer, asimismo, el protagonismo del Consejo de Seguridad de las Naciones Unidas a la hora de dirimir si un ciberataque es un ataque armado. Este protagonismo redundará, igualmente, en la delimitación conceptual del ciberataque, de conformidad con la legalidad internacional. En tanto este concepto no quede expresamente reflejado en la legalidad internacional, es evidente que el Consejo de Seguridad de las Naciones Unidas tendrá que pronunciarse de forma individualizada en cada caso, atendiendo a las específicas circunstancias que en cada ciberataque se presenten. De este modo, después de los pronunciamientos particulares por el Consejo de Seguridad de las Naciones Unidas, podrá alcanzarse la delimitación del concepto de ciberataque armado con carácter general y, en consecuencia, se podrá contar con un concepto aplicable, con carácter general, a los ataques informáticos que se produzcan en el futuro.

A la misma conclusión ha de llegarse cuando el ciberataque se utilice como método de combate, en el ámbito de la OTAN y de la UE. La expresa sumisión del Tratado de la OTAN a la Carta de Naciones Unidas impide que el Consejo Atlántico califique un ciberataque como ataque armado, sin tener en cuenta el

concepto que del mismo tengan las Naciones Unidas. Por lo tanto, en el supuesto de que los Estados que pertenecen a la OTAN se hallen en la necesidad de hacer uso o amenaza de la fuerza es aconsejable que el concepto de ataque sea delimitado por el Consejo Atlántico, en cada caso, y conforme a las exigencias que se hayan establecido por el Consejo de Seguridad de Naciones Unidas. Bien es cierto que el Tratado de la OTAN tiene por objeto, principalmente, establecer una alianza defensiva entre sus Estados miembros y, por lo tanto, estas cuestiones alcanzarán plena relevancia en el ámbito de la legítima defensa. Sin embargo, la activación de la legítima defensa colectiva que se en el ámbito de la OTAN requiere, en primera instancia, una delimitación del concepto de ataque que no ofrezca dudas a los Estados parte. En consecuencia, la adopción, por parte de la OTAN del concepto restrictivo que se propone, redundará, igualmente, en el respeto a la legalidad internacional, a través de esa preeminencia que se apuntaba y que hay que otorgar al Consejo de Seguridad.

Idénticas conclusiones se alcanzan del estudio del uso de la fuerza por parte de la UE, en virtud de la "cláusula de asistencia mutua" contenida en el TUE. También en este caso, hay que partir del concepto de ciberataque armado que establezca el Consejo de Seguridad de Naciones Unidas, pues únicamente de este modo, podrá hacerse efectivo el respeto a la Carta de Naciones Unidas que contempla el artículo 42.7) del TUE, que recoge dicha cláusula.

Se impone, por lo tanto, un concepto restrictivo que, también, tiene que ser defendido en el conflicto armado no internacional. De otro modo, determinadas actividades que se desarrollan a través de la red, de forma concertada y con un cierto grado de violencia o agresividad, podrían caer dentro del concepto de ataque armado, sin que, en realidad, llegaran a traspasar el llamado "*umbral de violencia*" que permite distinguir los disturbios internos del conflicto armado no internacional.

Además, esta restrictividad viene avalada por la consideración de internet como arma de doble uso. La posibilidad de que la red sea objeto de aprovechamiento lícito es tan incuestionable como que puede constituir un método de combate y estas características permiten afirmar que nos encontramos

ante un arma de uso dual. Por lo tanto, únicamente, cuando se produzca la utilización de este elemento en el conflicto armado, como método de combate, se tienen que establecer claramente sus condiciones de uso conforme a la legalidad y, nuevamente, quedarán fuera de este concepto el resto de actuaciones.

El contexto en el que se utilice internet no será un criterio determinante, pues, en un conflicto bélico, internet seguirá utilizándose de manera dual. No puede obviarse que, en los conflictos armados internacionales y no internacionales la red será objeto de uso, sin que ello suponga el empleo de un método de combate. Las comunicaciones de las Fuerzas Amadas de un Estado, durante el conflicto, tendrán lugar, cada vez con mayor frecuencia, a través de internet y esta actividad no supondrá por sí misma, el lanzamiento de un ciberataque armado. Esta circunstancia avala también la propuesta sobre la necesidad de una delimitación conceptual del ciberataque y cobra una mayor relevancia cuando el uso de internet se produce en el contexto de un conflicto armado.

SEGUNDA: El DIH es aplicable a los ciberataques como método de combate, como se desprende de los precedentes que han dado solución a las lagunas jurídicas producidas como consecuencia de la aparición de otros métodos de combate.

La novedad que supone la contemplación de los ciberataques como método de combate puede asimilarse a la que, en su día, se produjo en relación a las armas químicas, bacteriológicas o nucleares. Es decir que, si bien no contamos con precedentes en relación con la ciberguerra, sin embargo, la legalidad internacional cuenta con varios precedentes, en relación con la regulación jurídica de estas otras armas de doble uso. Por eso, es necesario tomar como referencia la práctica adoptada en el pasado en relación a situaciones que son similares, desde el punto de vista jurídico, a la que, en este momento, plantean los ciberataques.

En este sentido, hay que abogar por la aplicación del DIH al método de combate cibernético y abandonar la aspiración de una regulación convencional como la que rige las armas químicas o bacteriológicas. Esta regulación, pese a

dirigirse a un arma de la misma naturaleza que la que aquí se trata, sin embargo, no permite una traslación automática de sus propuestas. Los Convenios relativos a las armas citadas, parten de la base de un régimen de inspecciones y verificación que, en el ámbito cibernético supondrían una dificultad adicional y no tanto una solución. Parece que dichas actividades, en algún momento han de reflejar una actividad física que, en este caso, sería inviable. Por otra parte, no puede olvidarse que el control de estas otras armas descansa, en buena medida en la voluntad de los Estados.

Por lo tanto, cuando internet sea utilizado como un método de combate, durante el conflicto armado, deberá sujetarse al llamado "*imperativo de humanidad*"; es decir, a la aplicación de los principios que rigen todo conflicto armado. Tal y como ocurrió al suscitarse la necesidad de regular el uso de las armas nucleares, internet deberá someterse a la aplicación de los principios de DIH establecidos por la CIJ, en su Opinión Consultiva de 8 de julio de 1996. La aplicación de los principios relativos al combate que la CIJ denomina "inconculcables" o "cardinales" será obligatoria, por lo tanto, cuando el combate se desarrolle a través de métodos de combate cibernéticos.

Este sometimiento a los principios que rigen todo conflicto armado supone un argumento adicional a la defensa de un criterio restrictivo. En realidad, esta sumisión a las normas y principios de DIH solo podrá darse cuando nos encontremos ante un ciberataque armado y no en los casos en que internet se utilice de manera pacífica ni tampoco cuando, siendo ilícito su uso, no constituya un verdadero ataque armado, sino un ilícito encuadrable, por ejemplo, en el ámbito penal o antiterrorista.

La sumisión a los principios de DIH se dará en cualquier contexto en que el ciberataque se presente. El ciberataque armado presenta la singularidad de que puede manifestarse en contextos bélicos diversos. Es decir, un ciberataque podrá producirse aisladamente sin que, todavía exista el conflicto y ser, de este modo, un factor potenciador del mismo. Asimismo, podrá consistir en una ciberoperación que se desarrolle en el conflicto, junto con otras operaciones en las que se utilicen otros métodos de combate convencionales. Por último, aunque

con menor probabilidad, podrán lanzarse ataques armados entre Estados en conflicto que constituyan el único método de combate porque dichos Estados se encuentren librando una ciberguerra. En todos los casos, deberán aplicarse los postulados restrictivos que aquí se defienden y en todos ellos, igualmente, será de aplicación el DIH.

TERCERA: Un ciberataque contrario al DIH, será un método de combate prohibido y, por lo tanto, constituirá un hecho ilícito.

La novedad del hecho ilícito, tampoco en este caso permite abandonar el cumplimiento de la legalidad internacional. De las premisas hasta ahora expuestas, se concluye que, en determinados supuestos, el ciberataque constituirá un ataque armado. Por lo tanto, cuando dicho ciberataque armado sea lanzado en el contexto de un conflicto armado será de aplicación el DIH. En consecuencia, la infracción de las obligaciones internacionales impuestas por el DIH, originará la comisión de un hecho ilícito internacional.

En este ámbito resulta aplicable lo dispuesto en el artículo 2 del Proyecto, en relación a la comisión del hecho ilícito, tanto por acción como por omisión. Esto implica que, una vez más, el concepto de ciberataque armado tiene que ser restrictivo. De otro modo, la comisión del hecho ilícito por acción se podrá constatar erróneamente en los casos que ya se han citado y, además, implicaría un mayor riesgo al evaluar la omisión del Estado.

La omisión del Estado, al no impedir un ciberataque que infrinja el DIH, en el contexto de un conflicto amado internacional o no internacional, supondrá la violación de una obligación internacional. Sin embargo, para la apreciación del hecho ilícito por omisión será necesario evaluar determinados condicionantes que exigen también la adopción de criterios estrictos. En primer lugar, será preciso valorar si las medidas de aseguramiento de las redes informáticas han sido suficientes por parte del Estado. La obligación del Estado de garantizar la seguridad cibernética a sus ciudadanos, respecto de ataques que pudieran sufrir durante un conflicto armado, no puede ser absoluta. De otro modo, nos

encontraríamos ante situaciones en las que el Estado, sin tener capacidad para ejercer dicho control podría verse sometido a responsabilidad internacional.

En el caso de que la omisión se produzca durante el desarrollo de un conflicto armado, como consecuencia de la inacción de las Fuerzas Armadas, será necesario que los componentes de dichas Fuerzas Armadas, previamente, hayan obtenido una formación adecuada en relación a las normas de DIH aplicables al combate. Es decir, que quienes estén encargados de desarrollar las ciberoperaciones, hayan alcanzado un conocimiento de las cuestiones específicas aplicables al ciberataque como método de combate suficiente para conocer el alcance y contenido de dichas normas. Únicamente de este modo podrá evitarse el incumplimiento por omisión del Estado.

Se requiere, en consecuencia, que el adiestramiento en la materia sea adecuado porque la utilización de este método de combate, exige una interpretación del DIH adaptada al cibercombate. La obligación de impartir cursos de formación en DIH a los miembros de las Fuerzas Armadas debe cumplirse realizando una especial previsión sobre la interpretación del mismo en las ciberoperaciones. Los Mandos de las Fuerzas Armadas deberán formar a sus subordinados, advirtiéndoles de que el uso indebido de internet podría conllevar el lanzamiento de un ciberataque armado. Asimismo, sería conveniente una formación adecuada que previniera, a los miembros de las Fuerzas Armadas que presten servicio como operadores de redes informáticas, de las consecuencias que pudieran derivar de ello.

El cumplimiento de las normas de DIH impone, nuevamente, una interpretación restrictiva, pues resultará esencial transmitir la necesidad de cautela y, en consecuencia, adiestrar al personal en combate para evitar una calificación jurídica desproporcionada. Resulta imprescindible, por lo tanto, en este ámbito, establecer unos criterios que permitan distinguir en qué situaciones los ciberataques recibidos por las Fuerzas Armadas son calificados como ciberataques armados y, por lo tanto, susceptibles de dar lugar al hecho ilícito por omisión.

Esta necesidad de adiestramiento implicará, asimismo, formar al personal que, aunque no esté encargado del desarrollo de las ciberoperaciones, forme parte del Contingente en combate. Esta necesidad está motivada por el hecho de que estos componentes disponen de un sencillo acceso a la red, incluso desde dispositivos particulares. Es decir, la naturaleza dual de este arma impone, una vez más, la formación técnica y jurídica apropiada a todo el personal que, de una u otra manera, participe en un conflicto bélico.

Por otra parte, hay que tener presente que un Estado es también responsable de las omisiones de sus órganos, cuando existe el deber de intervenir; obligación que, en el conflicto bélico, se impone expresamente al Mando militar. En ese caso, podemos concluir que la omisión del Mando, cuando no actúe con la debida diligencia para evitar un ciberataque, que constituya una violación de las obligaciones impuestas por el DIH, originará el correlativo hecho ilícito por omisión del Estado, bajo cuya responsabilidad actúe.

En consecuencia, la necesidad de afrontar el combate con el adiestramiento adecuado exige que el mismo abarque la especificidad del elemento cibernético, más aún cuando el Proyecto de artículos extiende la responsabilidad internacional por el hecho ilícito al Estado, que preste ayuda o asistencia a otro Estado que cometa un ilícito internacional. Será en estos casos donde la formación deberá comprender, además, las actuaciones que se ejecuten en apoyo a Estados aliados en el desarrollo del combate.

CAPÍTULO SEGUNDO. EL CARÁCTER INTERNACIONAL DE LA OBLIGACIÓN DE DIH VIOLADA A TRAVÉS DE UN CIBERATAQUE. ORIGEN. VIGENCIA. CONTENIDO DE LA OBLIGACIÓN INTERNACIONAL.

1. INTRODUCCIÓN.

El contenido que en el presente Capítulo se aborda, pretende ofrecer una visión de la norma internacional violada a través de un hecho ilícito, tomando como presupuesto las conclusiones alcanzadas en el Capítulo precedente. Una vez afirmado que un ciberataque, utilizado como método de combate puede constituir un hecho ilícito, resulta obligado atender a la norma internacional que ha resultado violada a través de dicho ilícito activo u omisivo. En este sentido, el carácter internacional de la obligación se erige como eje central de la cuestión a abordar. Así, al examinar la obligación internacional infringida, será necesario determinar, con más detalle que en el Capítulo precedente, dicha naturaleza internacional. Para ello se continuará en el examen de la normativa convencional y consuetudinaria, sin olvidar los pronunciamientos de la jurisprudencia internacional.

Sin embargo, resulta aquí de especial utilidad, examinar todas aquellas actividades que, a priori pudiera confundirse con el uso de los ciberataques como método de combate. Es decir, partiendo de la base de que la actividad en internet puede ofrecer muy diversas manifestaciones, se hace preciso realizar una somera alusión a las que revisten mayor importancia o frecuencia, en orden a deslindar las mismas del objeto del presente estudio, así como a mencionar el ámbito jurídico en el que podrían quedar incursas. En este sentido, hay que hacer especial mención a actividades tanto lícitas como ilícitas que pueden desarrollarse con ocasión del uso de la red pero que, en modo alguno constituyen métodos de combate.

Conviene, en un primer momento, descartar determinadas actividades que no conllevan ningún riesgo, pues no puede concluirse que todo incidente

cibernético lleve aparejada una merma en la seguridad[186]. Igualmente, ante la imposibilidad de una regulación internacional y en ausencia de una gobernanza global de Internet, el ciberespacio ha visto un aumento de sus riesgos asociados a la seguridad de las sociedades avanzadas: el imparable incremento del cibercrimen, la utilización del ciberespacio por parte de grupos terroristas para ejecutar actividades de financiación, inteligencia, propaganda y captación, el ciberespionaje a gran escala entre Estados y/o empresas y el incremento de los delitos contra la privacidad de los usuarios en Internet son solo algunos de los retos a los que debe enfrentarse los responsables de las fuerzas de seguridad encargados de la ciberseguridad[187].

Este es el caso del llamado hacktivismo, es decir una actividad equivalente al activismo social, político o de cualquier otra índole que se manifiesta a través de la red y que, en ocasiones, por su magnitud o trascendencia puede originar confusión en cuanto a su tratamiento jurídico pero que en modo alguno puede equipararse a los ciberataques que se abordaban en el Capítulo Primero.

Asimismo, habrá que precisar el límite entre el terrorismo cometido a través de internet y el ataque armado, así como el distinto, en su caso, régimen jurídico aplicable, recogiendo el planteamiento formulado en el Capítulo Primero en relación a las conductas relativas a los insurgentes. Se trata aquí de entrar a ver en qué casos la respuesta a los actos de terrorismo ha de venir proporcionada por el Derecho interno y en qué supuestos dichos actos pueden ser cometidos en el desarrollo de un conflicto armado.

Por otra parte, no puede dejar de aludirse a los llamados ciberdelitos o cibercrímenes, cuya respuesta en el ámbito penal resulta clara y, a la vez,

186 Esta diferenciación queda clara cuando SINGER y FRIEDMAN afirman: "*Things may break and mistakes may be made, but a cyber problem only becomes a cybersecurity issue if an adversary seeks to gain something from the activity, whether to obtain private information, undermine the system, or prevent its legitimate use*". SINGER, P.W. y FRIEDMAN, A., *Cybersecurity and cyberwar. What everyone needs to know*, op. cit.; pp 34-39.

187 Así queda expuesto en el documento, REAL INSTITUTO ELCANO, *Las cibercelulas: una capacidad para la ciberseguridad y la Ciberdefensa nacionales*. ARI 26/2013, 4 de julio de 2013. Documento disponible en el sitio web: http://www.realinstitutoelcano.org/wps/wcm/connect/a68fc380403b31e089c3a9410786a7a3/ARI26-2013-THIBER-cibercelulas-ciberseguridad-ciberdefensa-nacionales.pdf?MOD=AJPERES. Fecha de consulta, septiembre de 2013.

ilustrativa de la necesidad del método interpretativo en relación a la necesaria delimitación conceptual.

Por último, en esta tarea de deslinde de conductas, habrá que hacer una breve alusión a los supuestos de ciberespionaje en orden a determinar, en qué supuestos ha de intervenir el Derecho Penal y en qué casos, las conductas de espionaje cometidas caen dentro del ámbito de aplicación del DIH y, por ende, susceptibles de constituir un hecho ilícito, conforme a lo antes expresado.

Una vez esclarecidas estas cuestiones, habrá que tener en cuenta que, aun habiendo sido aislado el estudio del ciberataque como método de combate, de las diferentes actividades aquí examinadas, hay que considerar que dicho ciberataque puede estar presente en diversos contextos. En este sentido, hay que tener en cuenta que los niveles de amenaza del ciberespacio y los sistemas y capacidades de ciberseguridad y ciberdefensa de los Estados no son homogéneos[188].

En este sentido, no puede olvidarse que "las Fuerzas Armadas dependen de las TIC para comunicarse, ejercer el mando y control de las operaciones, obtener y distribuir información e inteligencia, realizar labores de vigilancia, reconocimiento o adquisición de objetivos o coordinar los fuegos, con lo que las TIC actúan como multiplicador de la fuerza y optimizan la concepción, planificación y ejecución de las operaciones, pudiendo condicionar el desarrollo y resultado de una contienda"[189].

Así pues, partiendo de esta base, en la mayoría de los supuestos los ciberataques podrán estar presentes en una diversidad de situaciones que, en

188 Antes bien, en función del nivel de implantación y funcionalidad de sus sistemas nacionales de ciberseguridad y ciberdefensa, los países pueden agruparse en cuatro grandes grupos: Grupo 1, formado por aquellos países que disponen de un Sistema Nacional de Ciberseguridad y Ciberdefensa operativo, formalmente definido y en continuo proceso de evaluación, revisión y mejora. Este grupo estaría formado por países como EEUU, China e Israel; Grupo 2, formado por aquellos países que se encuentran en un proceso formal de construcción de sus sistemas nacionales de ciberseguridad y ciberdefensa. Este grupo estaría formado por países como Australia, Francia e Irán; Grupo 3, formado por aquellos países que se hallan en proceso de definición –formal o informal– de sus sistemas nacionales de ciberseguridad. Este grupo estaría formado por la gran mayoría de países, incluida España y Grupo 4, formado por aquellos países que todavía no han emprendido una definición –formal o informal– de su sistema nacional de ciberseguridad. REAL INSTITUTO ELCANO, *Las cibercelulas: una capacidad para la ciberseguridad y la Ciberdefensa nacionales*, doc. cit.

189 *Ibidem*.

todo caso pueden circunscribirse a tres contextos ineludibles en los que cabría resumir la gran mayoría de situaciones factibles: la ciberguerra, las ciberoperaciones y los ciberataques. Es decir, que los ataques informáticos utilizados como método de combate, podrán estar presentes en conflictos armados que se libren exclusivamente por medios cibernéticos o bien aparecer en combinación con otros métodos de combate o, por último, producirse con anterioridad al estallido del conflicto, hasta el punto de ser el desencadenante del mismo. En todos los casos, será necesario abordar el régimen jurídico aplicable a estos ataques informáticos en orden a determinar si en todas las situaciones descritas resulta o no aplicable la teoría del hecho ilícito que ha quedado expuesta y, en ese caso, cual es la norma de DIH que se infringe.

En este sentido, podrá darse el supuesto de que ese ataque cibernético se produzca en el transcurso de un conflicto bélico, de forma que la calificación jurídica que se le otorgue implicará la aplicación del llamado *ius in bello*, asimismo, convencional y consuetudinario. Aún más, en dicho contexto beligerante, el ciberataque podrá constituir una operación militar, desarrollada entre otras que podrían considerarse convencionales, o bien podrá resultar la única operación posible, por cuanto la misma se produce en el desarrollo de lo que ha venido a llamarse la "ciberguerra".

Por último, será preciso hacer referencia a los ciberataques como elementos potenciadores de un conflicto armado. Estos ciberataques, en determinadas circunstancias, podrán originar el estallido de un conflicto armado y, en función de su origen, éste conflicto, podrá ser internacional o no internacional. Igualmente, el comienzo del conflicto, podrá generar una ciberguerra o bien, un conflicto, convencional en el que se desarrollen ciberoperaciones. Así, el estudio de los ciberataques, como potenciadores de conflictos armados, permitirá concluir el estudio conceptual que se aborda, retomando la argumentación expuesta que resultará plenamente aplicable a estos frecuentes casos.

De cualquier modo, la delimitación conceptual de los distintos supuestos permitirá ofrecer la respuesta jurídica más acertada en un ámbito en el que, con

frecuencia, los conceptos son difusos y la respuesta a los hechos examinados no resulta clara.

Analizadas las diversas manifestaciones de los ataques cibernéticos y, teniendo en cuenta que éstos pueden ser considerados un método de combate, la invocación al DIH resulta inevitable.

En consecuencia, será necesario examinar cuál es el origen de dicha obligación de DIH y, por ende, ver de qué modo, tal como se expuso en el Capítulo precedente puede y debe aplicarse tanto el Derecho Convencional como el Consuetudinario. Por otra parte, es evidente que el carácter internacional de la obligación infringida, se deriva de su delimitación respecto de otro tipo de obligaciones, tales como las contractuales o las impuestas por el Derecho interno.

Asimismo, será preciso establecer en qué medida la obligación internacional que ha sido ya tratada en el Capítulo Primero y, a la que se ha dado la consideración de obligación *erga omnes,* puede ser considerada asimismo una obligación imperativa. Es decir, la naturaleza de las obligaciones de DIH determinará, como ya quedó apuntado, que nos encontremos ante obligaciones exigibles frente a todos los obligados, sea en virtud de una obligación convencional o consuetudinaria, o bien, que nos encontremos ante obligaciones cuyo cumplimiento resulta exigible por la comunidad internacional en su conjunto. De esta diferenciación en el origen y naturaleza de las obligaciones se derivarán, naturalmente, distintas consecuencias en el momento de plantear el mecanismo de responsabilidad internacional del Estado infractor.

La violación de la obligación internacional únicamente conllevará la responsabilidad del Estado en la medida en que su cumplimiento le resultara exigible en el tiempo. Es decir, cuando la obligación de que se trate esté vigente en el momento de cometer el hecho que pudiera reputarse ilícito. Pues bien, en este ámbito son varias las consideraciones que resultarán pertinentes, por cuanto, una vez más la idiosincrasia del método de combate cibernético obligará a replantear determinados presupuestos admitidos por la doctrina internacionalista y la Jurisprudencia internacional. La posibilidad, tantas veces apuntada, de programar en el tiempo un ataque informático y sus efectos,

conllevará el estudio de dichas posibilidades materiales a la luz de lo dispuesto en el Proyecto de artículos y su Comentario. Especial relevancia tendrá en este sentido, la consideración del ataque informático como hecho ilícito continuado y como hecho ilícito compuesto, es decir, integrante de un ilícito configurado con una multiplicidad de hechos.

Asimismo, resulta imprescindible atender al concreto contenido de la obligación internacional para, finalmente, determinar en qué supuestos se verá infringida la obligación internacional de DIH, sea ésta de origen convencional o consuetudinario y, bien se trate de una norma *erga omnes* o bien, imperativa. En esta materia habrá que atender a ese contenido al que se viene aludiendo, correspondiente al mínimo que ha de observarse en todo conflicto armado, sea internacional o no internacional y con independencia del método de combate que en el mismo sea empleado. Así, volviendo al método analógico se intentará desentrañar de qué modo las obligaciones más esenciales impuestas por la observancia del DIH, han de ser aplicadas a los ciberataques cuando éstos sean un método de combate en el transcurso de la ciberguerra o cuando se empleen como una ciberoperación.

En el acometimiento de dicha tarea se pondrá de relieve la existencia de una serie de principios ineludible o, en palabras de la CIJ, "inconculcables", que en todo caso han de ser respetados. Por ello, será preciso entrar a analizar de qué modo ha de respetarse la necesidad militar del ataque, cuando ese ataque sea lanzado por medios cibernéticos. Asimismo, habrá que entrar a analizar de qué modo la necesaria distinción entre civiles y combatientes, alcanza a los supuestos de ciberguerra y ciberoperaciones. Por otra parte, la especificidad del elemento cibernético obliga a tener presente la obligación de observar una proporcionalidad en el ataque, que impida la causación de daños innecesarios para la consecución del objetivo militar. Igualmente, resulta de especial relevancia atender a la prohibición de la perfidia, pues precisamente, el uso de la red permitirá el anonimato y enmascaramiento incluso de forma más evidente que los métodos de combate hasta ahora conocidos. Por último, en el examen del contenido de la obligación internacional de DIH infringida a través de un

ciberataque, resultará necesario hacer una alusión al respeto a la neutralidad de terceros, toda vez que la naturaleza virtual del medio informático planteará una nueva interpretación de dicho concepto.

Por ultimo y, de forma coetanea al studio del contendio de las obligaciones de DIH, se atendera al surgimiento de la relacion de responsabilidad internacional. Es decir, en coherencia con el contenido especifico de las obligaciones, se expondra la medida de reparacion a la que, el Estado infractor, podra quedar sujeto. A pesar de que el planteamiento de la cuetsion pueda parecer poco hortodoxo, al suponer una desviacion de la sistematica del Proyecto, sin embargo, la exposicion que se propone relaciona estrechamente los dos elementos. Es decir, el analisis de las cuetsiones relativas a la reparacion, como cosceuencia del hecho ilicto, no queda desligdo completamente del contendio de ese ilicito.

Así se hara referencia al contenido de la reapracion atendiendo a la obligacion de csacion y cumplimieto y a la necesidad de restituir al Estado lesionado, a la situación previa a la violación de la obligación internacional de que se trate.

Nuevamente, en el caso de violaciones de DIH por ciberataques, surgirán problemas en relación al cumplimiento de esta exigencia de restitución, porque, en ciertos casos, será necesario buscar la mas adecuada, hasta llegar a la indemnización y, en ultima instancia a las medidas de satisfaccion.

2. EL CARÁCTER INTERNACIONAL DE LA OBLIGACIÓN VIOLADA.

Como se ha analizado en el Capítulo Primero, el carácter internacional de la obligación violada está determinado por el contenido del artículo 12 del Proyecto que establece que "*Hay violación de una obligación internacional por un Estado cuando un hecho de ese Estado no está en conformidad con lo que de él exige esa obligación, sea cual fuere el origen o la naturaleza de esa obligación*." Así ha quedado

reconocido en constante Jurisprudencia internacional de que es reflejo la Sentencia dictada a resultas de conflicto en la embajada de Teherán[190].

En consecuencia, en los supuestos que aquí se abordan, puede afirmarse que la violación de una obligación internacional, impuesta por una norma de DIH, puede constituir un hecho ilícito internacional. Por lo tanto, no será posible calificar de internacionalmente ilícito un hecho, que suponga una contravención de obligaciones contenidas en contratos que se hayan celebrado, entre Estados y personas extranjeras o entre dos Estados, y que estén regidos por el Derecho interno de un Estado o, excepcionalmente, por un sedicente Derecho «transnacional»[191]. Tal y como aclara el Quinto Informe de la CDI, en relacion al Proyecto de articulos «*contracts are not agreements in which the contracting State or States participate as subjects of international law, and they are therefore in no way "international treaties*" »[192]. De este modo resulta tan relevante la existencia de una norma, como su aplicación al Estado en un caso concreto[193].

Una vez asumida la existencia de obligaciones *erga omnes*, en el ámbito de las relaciones internacionales, ha de concluirse que este tipo de obligaciones tienen cabida, en parangón a lo que ocurre en el Derecho interno. El carácter internacional de la obligación, asimismo, implica que la violación de una obligación puede contemplarse, tal como menciona el Informe de la CDI correspondiente a su 25ª sesión[194], como el equivalente a la idea de la *violación de los derechos subjetivos ajenos*.

---

190 Así lo entendió el Tribunal al establecer: "*Secondly, it must consider their compatibility or incompatibility with the obligations of Iran under treaties in force or under any other rules of international law that may be applicable. The events which are the subject of the United States' claims fall into two phases which it will be convenient to examine separately*". United States Diplomatic and Consular Staff in Tehran, doc. cit.; p. 26.

191 La cita queda recogida por PEREZ GONZALEZ en *La responsabilidad internacional (I): el hecho internacionalmente ilícito*, op.cit.; p. 7.

192 El documento continua afirmando, de forma taxativa: "*it is sufficient to emphasize that such contracts are not governed by the international legal order*". Fifth report on State responsibility by Mr. Roberto Ago, Special Rapporteur - the internationally wrongful act of the State, source of international responsibility (continued). Yearbook of the International Law Commission. 1976, vol.II. Doc. A/CN.4/291 and Add.1 & 2 and Corr. 1.; p.7, par.15.

193 Así puede leerse en el Comentario 13) al artículo 2 del Proyecto.

194 Report of the International Law Commission on the work of its twenty-fifth session, 7 May - 13 July 1973, Official Records of the General Assembly, Twenty-eighth session, Supplement No. 10. Doc A/9010/Rev.1.; p. 182; parr. 9.

En concreto, en el ámbito del DIH, se trata de unas obligaciones, cuyo propósito, es como como afirma el CICR, "*accorder un minimum d'humanité aux victimes des conflits armés constitue une responsabilité commune de tous les États et de tous les êtres humains* »[195].

Algunos autores, como MIAJA DE LA MUELA, al repecto, han señlado que "*la posibilidad de derechos absolutos en la vida internacional aparece así clara para quien no se encierre en una visión puramente voluntarista del derecho que la gobierna*"[196].

A mayor abundamiento, no puede olvidarse que, como afirma SALMON[197], "*las normas humanitarias codificadas no agotan todo el espectro de normas y principios humanitarios posibles*", sino que admiten pactos entre los Estados, pero únicamente cuando ello tenga como resultado un incremento en las garantías ofrecidas por el DIH[198].

En el mismo sentido ha tenido ocasión de manifestarse la Organización de Naciones Unidas, al entender que el hecho de responder a las graves violaciones que se cometan, en relación a los Convenios de Ginebra y su PA I, constituye una obligación para todos los Estados[199].

---

195 Dicha afirmación, queda confirmada por la jurisprudencia y, en este sentido, los referidos autores ponen de manifiesto, que «*un État qui encourage ou aide à la commission de violations par un autre État ou des forces dissidentes contrevient à l'article 1 commun. Les règles sur la responsabilité de l'État pour fait internationalement illicite précisent en outre qu'aucun État ne doit reconnaître comme licite une situation créée par une violation grave d'une norme impérative comme celles du DIH, ni fournir une quelconque aide ou assistance au maintien de cette situation*». SASSÒLI, M. ; BOUVIER, A.A.; QUINTIN, A. *Un droit dans la guerre?* Cas, documents et supports d'enseignement relatifs à la pratique contemporaine du droit international humanitaire. CICR, vol. I. Cap. 13; p. 21.

196 MIAJA de la MUELA, A., *Las situaciones jurídicas subjetivas en Derecho Internacional Público*, en Estudios de Derecho Internacional Público y Privado. Homenaje al Profesor Luis Sela Sampil. Universidad de Oviedo. 1970; pp. 25- 50, en particular; p.44.

197 SALMÓN, E. Introducción al Derecho Internacional Humanitario. Instituto de Democracia y Derechos Humanos. Pontificia Universidad Católica de Perú. CICR; p. 40.

198 Así lo pone de manifiesto la misma autora quien, sin embargo, también afirma que "*el propio artículo 3 común prevé la figura de los «acuerdos especiales» entre las partes en conflicto con el único propósito de mejorar y no perjudicar el trato a las víctimas, con lo que el mínimo contemplado no admite derogaciones sino que ostenta el carácter de compromiso absoluto para el Estado*" y que "*Los derechos salvaguardados por estas normas constituyen, por tanto, un conjunto mínimo irrenunciable que tiene como objetivo garantizar la protección de las personas protegidas por los cuatro Convenios de Ginebra*". SALMÓN, E. Introducción al Derecho Internacional Humanitario, op. cit.; p.36.

199 Las Naciones Unidas, así lo han entendido al expresar que: "*Regarding international armed conflicts, all States have the responsibility to respond to grave and other breaches of the Geneva Conventions and of Protocol I. Under the Geneva Conventions, States undertake the obligation to respect and to ensure respect for the Conventions in all circumstances. Specifically, States undertake to enact legislation to provide effective penal sanctions for perpetrators of grave breaches of international*

Pues bien, en consonancia con lo expresado hasta ahora, a la hora de formular la subsunción del hecho ilícito en la obligación internacional violada, habrá de tenerse en cuenta, únicamente, el Derecho Internacional.

Como consecuencia, la calificación del hecho no podrá verse afectada tampoco por la posible valoración que, del mismo hecho, pudiera realizarse por el Derecho interno[200], de modo tal que la conformidad con el Derecho interno no excluye que el hecho sea calificado como internacionalmente ilícito. Dicha conclusión puede, asimismo, alcanzarse a la vista del contenido del artículo 27 de la Convención de Viena, relativa a los Tratados Internacionales que dispone que "*Una parte no podrá invocar las disposiciones de su derecho interno como justificación del incumplimiento de un tratado*[201]." En el ámbito concreto, que aquí se estudia, tal supuesto ha sido, expresamente, contemplado en el ordenamiento interno español, de forma que el Código Penal tipifica como delito la violación de las normas de DIH[202].

Por lo tanto, advertido un ataque armado de las características que han sido expuestas, el Estado no puede invocar la ausencia de contravención con el Derecho interno para eximir su responsabilidad internacional. Idéntica solución cabría ofrecer en el supuesto de que dicho ataque se produjera con ocasión de un conflicto bélico, en el desarrollo de una ciberoperación.

Antes de comenzar a examinar las consecuencias, de la violación de la obligación internacional, en función del contexto en que se produzcan, los distintos ciberataques, es necesario realizar una serie de consideraciones que permitirán distinguir, con más precisión, aquéllos que se producen en el ámbito del conflicto bélico, de los que se producen en otro tipo de contextos.

Toda vez que, a lo largo de los últimos años, se ha producido una importante concienciación de las dimensiones, ventajas y peligros de las nuevas

---

humanitarian law". *International legal protection of human rights in armed conflict*. United Nations publication. New York and Geneva, 2011; pp. 82 - 84.

200 Así puede leerse en el artículo 3 del Proyecto y el Comentario 3) a dicho artículo.

201 Convenio de Viena sobre el Derecho de los Tratados, adoptado el 23 de mayo de 1969.

202 El Capítulo Tercero del Título XXIV del Código Penal, relativo a los delitos contra las personas y bienes protegidos en caso de conflicto armado, en sus artículos 608 a 614 bis, incorpora de forma profusa las conductas que el DIH prohíbe en el desarrollo del conflicto armado. Código Penal español, doc. cit.

tecnologías en el ámbito de la Seguridad Nacional, las ciberamenazas han sido incluidas como uno de los riesgos determinados y concretos que se recogen en la ESN 2013[203]. Como afirma ROBLES CARRILLO, "*El ciberespacio impone un nuevo paradigma de seguridad que encaja directamente en el propósito y el efecto de sustitución, característico de la fórmula «seguridad humana», más que en el modelo de ampliación material del objeto y los contenidos de la seguridad*[204]".

Esta es la primordial razón por la que resulta determinante, en cualquier estudio relativo a la seguridad cibernética, distinguir los ataques cibernéticos que se realicen en virtud de una motivación criminal, de aquéllos que pueden poner en peligro la Seguridad y Defensa del Estado que, a su vez, obligará a atender dos dominios diferentes y complementarios: la ciberseguridad y la ciberdefensa[205].

2.1. Delimitación de los ciberataques ilícitos a la luz del Derecho Internacional. La respuesta jurídica a distintas actividades en la red.

En el contexto que se viene exponiendo, las nuevas ciberamenazas han sido clasificadas en cinco áreas diferenciadas, en función de sus diversos fines u objetivos a los que, obviamente, habrá que dar una respuesta jurídica distinta,

203 Así queda puesto de manifiesto por AMICH ELÍAS, C. y VELÁZQUEZ ORTIZ, A.P. en el estudio llevado a cabo sobre las ciberamenazas en la Estrategia Nacional de Seguridad. AMICH ELÍAS, C. y VELÁZQUEZ ORTIZ, A.P., *La ciberdefensa y sus dimensiones global y específica en la Estrategia de Seguridad Nacional*, op. cit; pp. 49-76.

204 Asimismo, ROBLES CARRILLO realiza, en este sentido, una matización al entender que la afirmación anterior es susceptible de la siguiente diferencia: "*la ciberseguridad se está imponiendo, más que como una opción, por la fuerza de los hechos o por un principio de efectividad, mientras que la seguridad humana se ha movido, más y generalmente, en el plano de los ideales que en el de las realidades*". ROBLES CARRILLO, M. *El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico*. Documento de opinión 124/2015, 17 noviembre de 2015. Instituto Español de Estudios Estratégicos. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-Ciberseguridad_Margarita-Robles.pdf.; p.7. Fecha de consulta, enero de 2016.

205 La dicotomía que aquí se refleja, ha sido expuesta en AA.VV, Estrategia de la información y seguridad en el ciberespacio. Documentos de Seguridad y Defensa, núm. 60. Escuela de Altos Estudios de la Defensa. Ministerio de Defensa. Madrid. Junio 2014; pp. 13- 14.

adecuada y proporcionada. Estas cinco áreas son la ciberdelincuencia, el ciberterrorismo, el hacktivismo, el ciberespionaje y la ciberguerra[206].

Las antedichas categorías supondrán la base, desde la que se emprenda la tarea de la calificación jurídica, del ciberataque de que se trate en cada caso concreto pues, de otro modo, podría llegarse a conclusiones confusas, que ofrecieran respuestas, no sólo erróneas, sino desproporcionadas.

En el ámbito que aquí se atiende, es necesario acotar el estudio de los casos de cibercrímenes o de ciberterrorismo pues, estos casos, aun cuando pudieran revestir caracteres de ataque armado, no siempre incurrirán en dicha calificación jurídica, siempre dejando a salvo las consideraciones, que ya han sido realizadas en el Capítulo precedente, en relación a las actividades realizadas por insurgentes durante el conflicto, al margen del Estado. Es ésta una de las tareas de mayor complejidad por cuanto, la actuación de los ciberatacantes no siempre resultará fácilmente calificable. Antes bien, la difusa delimitación entre unos conceptos y otros impedirá, en muchas ocasiones, un acertado enfoque jurídico de la cuestión. Por tal motivo, en lo que al presente estudio concierne, procede la exclusión de las conductas que no constituyen, en última instancia un ataque armado, pero a las que en todo caso ha de darse una respuesta jurídica.

2.1.1 El hacktivismo y sus posibles implicaciones en la Seguridad nacional.

La actividad que se realiza a través de internet puede revestir diversas manifestaciones que incluyen aquéllas que, por novedosas, han suscitado dudas, pero que se han revelado como meras actuaciones tendentes a la actividad social y, por lo tanto, inofensivas. Así puede considerarse el llamado hacktivismo, cuyas manifestaciones engloban, desde hace tiempo, una gran cantidad de actuaciones que se desarrollan en la red[207].

206 Así se expresa HERNÁNDEZ GARCÍA, L. F., *Ciberseguridad; respuesta global a las amenazas cibernéticas del s. XXI. Las ciberamenazas, un nuevo reto para la Jefatura de Información de la Guardia Civil*. Cuadernos de la Guardia Civil núm. 49. 2014; pp. 5-35, particular, p. 12.

207 Como MAYORGA MARTÍN pone de manifiesto, el hacktivismo ha estado presente en la red prácticamente desde los comienzos de su funcionamiento, siendo, a título de ejemplo, alguna de sus manifestaciones, las siguientes: en octubre de 1989, mediante el uso del protocolo DECNET, un gusano llamado WANK (del inglés, Worms Against Nuclear Killers, gusanos contra los

De conformidad con los criterios ofrecidos en el Capítulo precedente, este tipo de actividades quedarán excluidas, en primer lugar, por la ausencia de violencia contra un objetivo, pues su intención, habitualmente, será la de llamar la atención ante una causa de carácter social o político. Con carácter general puede afirmarse que los objetivos atacados o la intensidad del ataque no permitirán indicar la existencia de un ataque armado. No obstante, como podrá verse en el epígrafe inmediatamente posterior, podremos encontrarnos con ataques cibernéticos, cuya inicial ausencia de ofensividad, desemboque en un conflicto, por tratarse de ciberataques potenciadores de un ulterior conflcito armado.

Asimismo, habrá que tener presente que, en función del bien jurídico protegido, que pudiera resultar atacado por dichos ciberataques, podría ser precisa la respuesta penal por parte del Estado. De este modo, podría darse el supuesto de que, como consecuencia de una actividad reivindicativa, la escalada de violencia, a través de los mensajes o actividad en la red, derivara en actos de ciberterrorismo, en sentido estricto, en delitos informáticos, o bien delitos comunes a través de medios informáticos. Nada de lo que aquí se plantea resulta puramente teórico pues, los ciberataques que sufrió Estonia en la primavera de

---

asesinos nucleares) se propaga por la red informática de la NASA en Maryland. Uno de sus objetivos era difundir un mensaje denunciando los peligros de los ensayos nucleares; en noviembre de 1994, Los "Yippies" lanzan un ataque de denegación de servicio distribuida (DDoS) y una campaña de envío masivo de correo a los servidores del gobierno británico para protestar contra una ley que prohíbe los conciertos de música con un ritmo repetitivo al aire libre; en diciembre de 1995, En Italia, el grupo Strano Network decide bloquear sitios web franceses para protestar contra los ensayos nucleares en Mururoa; en enero de 1998, En apoyo a las guerrillas zapatistas, se celebra una manifestación virtual en respuesta a una masacre cometida por fuerzas paramilitares en un pueblo de Chiapas, México; en diciembre de 1999, El grupo Electrohippies Collective organiza una sentada virtual, en la que todos sus seguidores deben visitar las páginas web de la Organización Mundial del Comercio para bloquear el comunicado final de la conferencia de Seattle, Washington, con el fin de impedir su difusión; en junio de 2001, al objeto de protestar contra el uso de los aviones de la compañía Lufthansa con el fin de deportar a inmigrantes sin papeles de Alemania, dos redes humanitarias alemanas organizan una protesta virtual para bloquear el sitio web de la aerolínea mediante el envío masivo de mensajes de correo electrónico. Éstas y otras actividades englobadas en el concepto de hacktivismo, son analizadas por MAYORGA MARTÍN, J.L., *Hacktivismo*. Cuadernos de la Guardia Civil. Número 49. 2014; pp. 36-53, en particular, p. 40.

2007, se produjeron como resultado de las protestas, de carácter político, que la minoría rusa en Estonia efectuó contra el Gobierno de aquél país[208].

En consecuencia, la actividad en la red, aun cuando se trate de mero activismo social, político, cultural o de cualquier otra índole, inicialmente carente de riesgo, puede derivar en una actuación que llegue a afectar a la Seguridad Nacional. Se hace preciso entonces atender al propio concepto de Seguridad Nacional que, en virtud de su dinamismo ha ido adaptándose a las necesidades que la sociedad ha demandado. Si la Seguridad Nacional, como afirma CARO BEJARANO, ha sido tradicionalmente configurada como aquélla que garantizaba la "*identidad y supervivencia nacionales*", actualmente incluye, como pone de manifiesto la misma autora, riesgos, como los provenientes de desastres naturales, el cambio climático, las tecnologías de la información y las comunicaciones[209].La interrelación, pues, entre los conceptos de seguridad y defensa es estrecha, por cuanto los factores que puedan amenazar a una u otra categoría, a menudo coinciden.

El concepto de Seguridad Nacional se halla, intrínsecamente, relacionado con la Defensa Nacional. A esta perspectiva respondería el concepto de seguridad que, para las Naciones, pretende garantizarse a través de la Carta de las Naciones Unidas y que se corresponde con la ausencia de la amenaza militar[210].

De modo evidente, cuando el elemento cibernético, tan presente en la vida cotidiana de los ciudadanos, a quien se procura esta Seguridad, es utilizado, como medio de expresión, comunicación o vehículo para transacciones

208 La cronología y el contexto social en que se produjeron estos incidentes, queda ampliamente reflejado en la obra, impulsada por la OTAN, con el titulo, International Ciberincidents. Legal considerations, que ha sido publicada por el CCDCOE de OTAN. Asimismo, en dicha se da cumplida cuenta de los ciberataques sufridos por Bielorrusia, Lituania y Georgia. TIKK, E. KASKA, K., VIHUL, L. International Cyberincidents. Legal Considerations. NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallin (Estonia), 2010. En concreto, en relación a los ciberataques constatados en Estonia; pp. 15 a 25.

209 Así se expresa CARO BEJARANO, M. J., en *Alcance y ámbito de la seguridad nacional en el ciberespacio. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, en Cuadernos de Estrategia núm. 149. Instituto Español de Estudios Estratégicos. Instituto Universitario «General Gutiérrez Mellado». Diciembre 2010; pp. 49-82.

210 SÁNCHEZ DE ROJAS DÍAZ, E. *Recursos vitales y recursos energéticos. Algunos conceptos básicos.* Recursos vitales y recursos energéticos. Implicaciones para la seguridad. Escuela de Altos Estudios de la Defensa. Monografías núm. 141. Septiembre 2014; pp. 19-62, en particular, p.22.

comerciales, entre otras, no puede quedar al margen de los factores integrantes del concepto de Seguridad Nacional.

Esta perspectiva de la Seguridad Nacional se sustenta, por lo tanto, en el mismo concepto de Estado, cuyo elemento territorial se ve ahora cuestionado, pues el Estado se encuentra en la obligación y necesidad de hacer frente a amenazas que proceden de un ámbito eminentemente virtual. No obstante, esta nueva percepción de la amenaza, proveniente de un ámbito, que no se circunscribe a los límites territoriales del Estado, no puede ocultar el hecho de que, el ataque en cuestión, siempre provendrá de un equipo informático radicado en algún lugar físico y que será lanzado, por un individuo, que detente una nacionalidad, por mas que todo ello pueda ser enmascarado, por el anonimato favorecido por la red.

Ambos conceptos de independencia e integridad territorial del Estado, presentes en el concepto de seguridad, ha llevado a algún autor a apuntar la necesidad de un incremento de las capacidades militares, que permita hacer frente a este tipo de nuevas amenazas[211].

Resulta, asimismo, obligado tener en cuenta que, las amenazas a la seguridad del Estado ya no provienen únicamente de otros Estados, sino también de individuos y que, de la misma manera, son éstos quienes, en gran parte de las ocasiones, son víctimas de los ciberataques producidos por otros individuos y, por lo tanto, son acreedores de la protección y seguridad que ha de prestar su Estado[212]. De esta forma, se ha acuñado el concepto de «*seguridad humana*» que pretende recoger la novedosa caracterización de los problemas de seguridad, pasándose de la visión estatocéntrica clásica, a las visiones que se centran en un nivel global o individual[213].

En el ámbito que ahora nos ocupa, la ciberseguridad ha sido entendida como aquélla que se garantiza en el ámbito de los medios informáticos y resulta esencial, no sólo para la protección del individuo, sino también de la economía

211 De esta forma recoge SÁNCHEZ DE ROJAS DIAZ, la definición aportada por PÉREZ DE ARMIÑÓN. SÁNCHEZ DE ROJAS, en *Recursos vitales y recursos energéticos. Algunos conceptos básicos,* op.cit.; p. 23.
212 *Ibidem*; pp. 23-24.
213 *Ibidem;* pp. 22-24.

global, las operaciones militares y la infraestructura crítica[214]. Puede afirmarse, por lo tanto, que la Seguridad Nacional, entendida como el concepto equivalente a la exención de peligro, de daño o de riesgo, se contempla desde una perspectiva que incluye diversos elementos, como son los ámbitos militar, político, económico, social y medioambiental.

2.1.2. La Ciberdelincuencia.

Las actividades relacionadas con la delincuencia y el terrorismo han alcanzado un mayor protagonismo y relevancia, desde que pueden ser cometidos, por medios cibernéticos. Si bien su tratamiento jurídico puede entenderse resuelto, *a priori*, en el ámbito interno, no es menos cierto que, ambos supuestos, ya no son considerados meros riesgos, sino verdaderas amenazas equiparadas, en este sentido, a la amenaza que, para un Estado puede suponer un ataque de las Fuerzas Armadas de otro Estado[215]. La interrelación entre ambos fenómenos es tan sumamente estrecha, que algunos autores han puesto de manifiesto el hecho de que, el crimen organizado puede ser factor potenciador de conflictos, así como que, el conflicto armado, a su vez, puede originar el desencadenamiento de la delincuencia organizada.[216]

Se trata de un tipo de amenaza que no puede considerar eventual o, meramente posible, sino probable, habida cuenta la alta y sencilla disponibilidad

214 Así se expresa SÁNCHEZ DE ROJAS en el artículo publicado en la Revista Ejército. SANCHEZ DE ROJAS DIAZ, E. *¿Ciber…qué?. La ciberseguridad., retos, riesgos y amenazas*. Revista Ejército núm. 837. Diciembre 2010; pp. 136- 143.

215 Asi lo entiende GONZALEZ CUSSAC, cuyo razonamiento puede encontrarse en GONZÁLEZ CUSSAC, J. L., *Estrategias legales frente a las ciberamenazas*. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, en Cuadernos de Estrategia, núm. 149. Instituto Español de Estudios Estratégicos. Instituto Universitario «General Gutiérrez Mellado». Diciembre 2010; pp. 79-127, en particular, p.30.

216 DE LA HOZ CABALLER, en este sentido, afirma: "(…) *frente a una situación de crimen organizado generalizado y descontrolado un Estado puede aplicar, para su resolución, estrategias militares que devenguen en un conflicto abierto entre la organización criminal, si tienen fuerza suficiente, y el propio Estado.*"; "(…) *la desorganización social desemboca en una «organización o asociación diferencial», es decir, el vacío de poder de un Estado inoperante es aprovechado por las organizaciones criminales para imponer su actividad y establecer una suerte de organización alternativa* (…)". DE LA HOZ CABALLER, J. *Criminalidad y conflicto*. Nuevas guerras nuevas paces, en Monografias del CESEDEN, núm. 131. Centro Superior de Estudios de la Defensa Nacional. Septiembre 2012; pp. 295-341, en particular, pp.313-322.

que, del uso de la tecnología, pueden realizar, tanto los Estados como los individuos. Cuando estas amenazas se han materializado, han obligado a un nuevo replanteamiento del concepto de Seguridad Nacional. Si hasta ahora ha podido verse cómo la Seguridad nacional ha tratado de proteger al propio Estado, frente a ataques externos, garantizando así la soberanía, independencia e integridad territorial, dicho concepto ha tenido que ser reconfigurado, en orden a ofrecer esa misma seguridad, al individuo. Todo ello sin olvidar que, como se ha visto en el Capítulo precedente, en el desarrollo de la nueva tipología de los conflictos armados, es el individuo, el que puede poner en entredicho la Seguridad del Estado.

El Derecho Penal ha dado respuesta a una serie de fenómenos delictivos o modalidades comisivas que, en gran medida, ha venido a cubrir la laguna legal que, en este campo se produjo, con la irrupción de las nuevas tecnologías[217]. De esta forma, podemos encontrar un primer grupo de actuaciones tipificadas, que se relacionan con la propia existencia de internet y que protegen, tanto el uso de la red, como el de los equipos o dispositivos informáticos[218]. Por otra parte, otras conductas, que ya eran objeto de sanción penal, con anterioridad a la irrupción de medios cibernéticos, han visto alterada su modalidad comisiva, gracias al uso de dichos medios. También en estos casos, la nueva modalidad comisiva ha encontrado su correspondiente respuesta penal[219].

---

217 La regulación del delito en la red y sus distintas modalidades comisivas, es objeto de un detallado estudio por parte de FERNANDEZ RODERA. FERNANDEZ RODERA, J.A. *La lucha contra el delito en la red*. Revista Cuadernos de la Guardia Civil núm. 51, 2015; pp. 112-123.

218 De este modo, el Código Penal ha recogido conductas socialmente reprochables, esencialmente relacionadas con el uso de las nuevas tecnologías, como por ejemplo, el delito de daños cualificados del apartado primero del artículo 264 del Código Penal, en el que se castiga a quien «(…) *sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos* (…)»; así como las recogidas en el párrafo segundo del mismo artículo, que establece la responsabilidad penal de quien «(…) *sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos* (…)».

219 Como ejemplos más relevantes, cabe citar la comisión de estafa, prevista y penada en el artículo 248 del Código Penal "(…) *valiéndose de alguna manipulación informática o artificio semejante* (…)"; o los actos contra la indemnidad sexual de menor de trece años a través de Internet, del teléfono o de cualquier otra tecnología, penados en el artículo 183 bis.

En este ámbito, ha resultado de especial significación la labor realizada por la Jurisprudencia pues, con carácter previo a la tipificación de determinadas conductas o, incluso, para considerar determinados hechos, contenidos en el tipo de lo injusto, ha sido necesaria la interpretación de determinados conceptos a la luz de la nueva realidad[220].

Asimismo, las garantías constitucionales se han visto afectadas, por el uso de este tipo de comunicaciones y, de esta manera, el Tribunal Constitucional ha entendido que, la comisión de determinados delitos por medios cibernéticos puede justificar, entre otros motivos, la limitación del derecho a las comunicaciones.[221]

Éstos son sólo algunos de los ejemplos que pueden hallarse en el Derecho interno[222] y que, en cualquier caso, resultan ilustrativos de la necesidad de delimitación conceptual en la materia y de la oportunidad de aplicar, en dicha tarea, la interpretación analógica. Este uso de la analogía, como se verá posteriormente, resulta, asimismo, necesario a la hora abordar las consecuencias jurídicas, del empleo de los ciberataques, como método de combate.

---

220 Un claro ejemplo de ello, es el concepto de documento cuya adaptación a los nuevos soportes informáticos se realizó tal y como expresa el Tribunal Supremo: "*(…)Si bien es cierto que ese concepto de documento ha sido clarificado en el artículo 26 del vigente Código de 1995, no lo es menos que durante la vigencia del anterior también se consideró que los soportes informáticos podían ser objeto de falsedad penal, y así tenemos que la sentencia de esta Sala de 24 de noviembre de 1997 , que se apoya a su vez en las sentencias de 3 de junio y 11 de octubre de 1994, nos indica que ha de entenderse por documentos a esos efectos, no sólo el escrito plasmado en papel según el criterio tradicional, sino también todo aquello que se le pueda asimilar, por ejemplo, un disquete, un documento de ordenador, un vídeo, una película, etc., «con un criterio moderno de interacción de las nuevas realidades tecnológicas en el sentido en que la palabra documento figura en algunos diccionarios como cualquier cosa que sirve para ilustrar o comprobar algo (…)*". Sentencia número 1844/2000 de 2 diciembre, de la Sala de lo Penal del Tribunal Supremo.

221 Las razones son expuestas por el Tribunal Constitucional en sentencia núm. 104/2006 de 3 abril de 2006, del siguiente modo: "*(…) En estas circunstancias, en las que se pone de manifiesto que la policía judicial intentó la investigación de los hechos por otras vías alternativas menos gravosas sin éxito, durante cinco meses –del 24 de marzo al 31 de agosto de 2000–, y en las que la utilización de las tecnologías de la información a la vez que facilitan la comisión del delito dificultan su persecución, no puede sostenerse que la investigación de un delito contra la propiedad intelectual cometido mediante la utilización de las tecnologías de la información carezca de la entidad necesaria para considerar desproporcionada la intervención de la línea del teléfono móvil de contacto que aparecía en la página web en la que se ofertaban los productos informáticos. En definitiva, en el juicio de proporcionalidad de la interceptación de las comunicaciones telefónicas, además de la gravedad de la pena, del bien jurídico protegido y de la comisión del delito por organizaciones criminales, también puede ponderarse la incidencia del uso de las tecnologías de la información, pues su abuso facilita la perpetración del delito y dificulta su persecución (…)*".

222 Por la propia naturaleza del presente trabajo, sólo algunos de los ejemplos que se han considerado más relevantes, han sido aquí incluidos. Un estudio más detallado sobre el particular puede encontrarse en GONZÁLEZ CUSSAC, J. L., *Estrategias legales frente a las ciberamenazas*, op.cit.; pp. 85-127.

Una importante labor en esta tarea tendente a la definición y tipificación de las nuevas conductas penales, ha sido llevada a cabo en el ámbito del Derecho Internacional, por parte del Convenio Europeo sobre Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001. A la luz de lo dispuesto en el Informe Explicativo[223] aprobado por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el Convenio tiene, como finalidad primordial, armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada Estado y las disposiciones conexas en materia de delitos informáticos; establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico y establecer un régimen rápido y eficaz de cooperación internacional.

En lo que respecta a los comportamientos que, necesariamente, han de ser configurados como ilícitos penales en las correspondientes legislaciones internas, se estructuran en las siguientes categorías: las Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos informáticos. En este grupo se deben describir, como infracciones penales, el acceso ilícito doloso y sin autorización a sistemas informáticos; la interceptación dolosa e ilícita, sin autorización, a través de medios técnicos, de datos informáticos, en el destino, origen o en el interior de un sistema informático; los atentados contra la integridad de los datos, consistente en dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos; los atentados contra la integridad del sistema, esto es, la obstaculización grave, dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos; el abuso de equipos e instrumentos técnicos, que comporta la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de dispositivos principalmente concebidos o

223Convenio sobre la Ciberdelincuencia. Firmado en Budapest el 23 de noviembre de 2001. Informe Explicativo al Convenio sobre la Ciberdelincuencia. Consejo de Europa. STE núm. 185.

adaptados para cometer las infracciones antes referidas; la de una palabra de paso (contraseña), de un código de acceso o de datos similares que permitan acceder a un sistema informático; y la posesión de alguno de los elementos antes descritos.

El segundo de los grupos, está constituido por las Infracciones informáticas y, entre ellas, según el Convenio, deben sancionarse las falsedades informáticas, que contienen la introducción, alteración, borrado o supresión dolosa y sin autorización, de datos informáticos, generando datos no auténticos; la estafa informática, que precisa la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de la introducción, alteración, borrado o supresión de datos informáticos, o de cualquier otra forma de atentado al funcionamiento de un sistema informático, siempre con la intención fraudulenta, de obtener un beneficio económico.

Asimismo, un tercer grupo, incluye las Infracciones relativas al contenido, entre las que se incluyen las conductas relativas a pornografía infantil.

Por último, se contienen las Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

En conclusión, la comisión de las conductas que se contienen en nuestro ordenamiento interno, como reflejo de lo dispuesto en el Tratado, firmado por España supone la comisión de un delito cibernético o de un delito común, cometido a través o valiéndose de medios virtuales, y, por lo tanto, entrará en el ámbito del Derecho Penal. El Derecho Penal, así, prevé la adecuada respuesta a dichas actividades sin que, por ende, puedan ser confundidas estas actuaciones, con las que eran definidas en el Capítulo Primero como ataques armados.

2.1.3 El Ciberterrorismo.

El terrorismo cibernético o las actuaciones de dicha índole, propagadas a través de la red, han supuesto una novedad en las relaciones entre los Estados, de tal envergadura, que requieren un estudio detenido acerca del tratamiento jurídico de estas actuaciones. Como se ha puesto de manifiesto por diversos

autores, "*el terrorismo cibernético representa una grave amenaza para la seguridad económica y de las naciones*" [224]. Así, a pesar de que, en realidad, no se tiene conocimiento de un auténtico atentado terrorista cometido a través de la red, sin embargo, determinados movimientos terroristas, han aprovechado la existencia de la red para la consecución de sus propósitos, de tal modo que "*La expansión de internet ha cambiado drásticamente la estructura y el desarrollo de la amenaza del terrorismo global islamista*"[225]. De este modo, como afirma CARLINI, a diferencia de otros grupos terroristas, el ISIS "*demuestra una fuerte capacidad de adaptación a las tecnologías del siglo XXI. Las redes sociales, como Facebook, YouTube, Twitter o Instagram han jugado un papel muy importante en el proceso de reclutamiento de nuevos terroristas*[226]"

En una primera aproximación, no parece que este tipo de terrorismo pueda tener la consideración de ataque armado que ha sido expuesta en el Capítulo Primero, pues el componente virtual, hasta la fecha ha jugado un papel limitado. En efecto, internet constituye un medio de comunicación que incrementa notablemente la necesidad de propaganda que todo grupo terrorista tiene. Por otra parte, siendo ésta la labor fundamental de la red para las organizaciones terroristas, no puede olvidarse que no es éste su único uso. Antes bien, grupos terroristas de carácter islámico como el ISIS, se valen del entorno virtual para realizar actividades que WEIMAN ha identificado como de guerra psicológica, de publicidad y propaganda, extracción de datos, recaudación de fondos, reclutamiento y movilización, trabajo de red, información compartida y planificación y coordinación[227]. Es decir, a través del uso de internet, parece que

224 CARLINI, A. *Isis: una amenaza en la era digital*. Instituto Español de Estudios Estratégicos. Documento de Opinión 129/2015. 1 de diciembre de 2015; p.3. Documento disponible en el sitio web: Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-2015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf. Fecha de consulta, enero 2016.

225 TAPIA ROJO, M.E., *Análisis de la estrategia comunicativa del terrorismo yihadista: el papel de las redes sociales*. Instituto Español de Estudios Estratégicos Documento de Opinión 02/2016. 4 de enero de 2016; p. 4. Disponible en el sitio web: Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO02-2016_Comunicacion_ISIS_EugeniaTapia.pdf. Fecha de consulta, marzo de 2016.

226 CARLINI, A., *I Isis: una amenaza en la era digital*.doc. cit; pp. 7 y 8.

227 Esta enumeración realizada por WEIMAN es recogida, con mayor detalle, en el Documento de Opinión ya citado, CARLINI, A., *I Isis: una amenaza en la era digital*.doc. cit; pp. 4 y 5.

las actividades que eran, tradicionalmente, propias de los grupos terroristas, se realizan, en la actualidad, valiéndose de un único instrumento que, además proporciona o, al menos, facilita la inmediatez y el anonimato. De esta manera, puede llegar a hablarse de ciber terrorismo, entendiendo que el mismo abarca las actuaciones que se han enumerado y no, hasta la fecha, la realización de ningún ciber atentado.

No obstante, en el supuesto de que ello llegara a darse, habría que tener presente que la calificación jurídica de los actos de terror resulta siempre especialmente compleja. No cabe duda de que cualquier conducta relacionada con la actividad terrorista tendrá su encaje en el ámbito penal, que ha sido ya examinado, pero conviene, en este punto, recordar que, la frecuencia con que se presentan los conflictos de carácter asimétrico, obliga a tener en cuenta que el insurgente o terrorista puede llegar a tener la condición jurídica de combatiente. En este sentido el CICR, recuerda que "*La mayoría de las medidas adoptadas por los Estados y otras entidades para prevenir o suprimir los actos de terrorismo no equivalen a un conflicto armado en el sentido práctico ni jurídico*[228]" y, en consecuencia, el CICR no reconoce el estatuto de combatiente a quien comete actos terroristas y, además ha dejado claro que "*los grupos " terroristas " que actúan por cuenta propia y sin el vínculo necesario con un Estado o una entidad similar están excluidos de las protecciones que amparan a los prisioneros de guerra*[229]".

A los efectos que aquí se tratan y, como se verá en el Capítulo correspondiente, esa asimetría del conflicto obligará a plantear si la conducta del ciber terrorista se debe atribuir, exclusivamente al individuo o, por el contrario, al Estado le puede resultar exigible la responsabilidad internacional correspondiente a dicha actuación.

En la medida en que dichas actuaciones, de naturaleza terrorista sean llevadas a cabo por el Estado, ha de ser considerada la valoración que realiza el

228 Así puede leerse en¡, CICR, *Desafíos del DIH: el terrorismo*. Documento de 29 de octubre de 2010. Disponible en el sitio web: https://www.icrc.org/spa/war-and-law/contemporary-challenges-for-ihl/terrorism/overview-terrorism.htm#header. Fecha de consulta, junio de 2013.

229 Estas son las conclusiones que pueden encontrarse en el documento del CICR, *La pertinencia del DIH en el contexto del terrorismo*, de 1 de enero de 2011. Disponible en el sitio web www.icrc.org/spa/resources/documents/misc/6fsjl7.htm#header. Fecha de consulta, junio de 2013.

DIH sobre los actos de terror, al establecer en la Norma 2 de la Compilación de DIH consuetudinario que "*Quedan prohibidos los actos o las amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil*"[230]. La Norma transcrita no es sino un reflejo de la contenida en el DIH Convencional que, en el párrafo 2 del artículo 51 del PA I prohíbe la realización de "*actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil*". Idéntico contenido puede encontrarse en el artículo 33 del IV Convenio de Ginebra que, asimismo prohíbe "*toda medida de intimidación o de terrorismo*". Por último "*los actos de terrorismo*" aparecen también expresamente prohibidos en el artículo 4, párrafo 2 del PA II[231].

Sin embargo, las antedichas prohibiciones, no hallan su encaje en las actuaciones que se desarrollan en el transcurso del combate. El CICR dice que "*Independientemente de las motivaciones de sus autores, los actos terroristas cometidos fuera de un conflicto armado incumben al derecho nacional y al derecho internacional, y no al derecho de la guerra*[232]". Antes bien, tienen como misión prohibir los actos de terrorismo cuando éstos sean utilizados "*como medio para mantener o conseguir el orden y la seguridad en los territorios ocupados o en la población que tienen las partes beligerantes en su poder*[233]" y se entienden por tales,

---

230 HENCKAERTS J.-M., DOSWALD-BECK, L. Customary International Humanitarian Law, vol. II. Practice Part 1. International Committee of the Red Cross 2005, Cap. 1.; pp. 9 - 12.

231 Como ejemplos de la práctica de estas normas, el CICR, cita las siguientes: "*556. In an appeal issued in October 1973, the ICRC urged all the belligerents in the conflict in the Middle East (Egypt, Iraq, Israel and Syria) to observe forthwith, in particular, the provisions of, inter alia, Article 46(1) of draft AP I, which stated that "methods intended to spread terror among the civilian population are prohibited". All governments concerned replied favorably. 557. In a communication to the press in 1993, the ICRC reminded the parties to the conflict in Nagorno-Karabakh that "acts of violence intended to spread terror among the civilian population are also prohibited". 558. In 1994, in a Memorandum on Respect for International Humanitarian Law in Angola, the ICRC stated that "all acts or threats of violence the main purpose of which is to spread terror among the civilian population are also prohibited.(…) 561. In a communication to the press in 2000 concerning the violence in the Near East, the ICRC stressed that "terrorist acts are absolutely and unconditionally prohibited*". HENCKAERTS, J.-M., DOSWALD-BECK, L. Customary International Humanitarian Law, vol. II. Practice Part 1, op. cit.; parr. 556 - 558 y 561; pp.76 y 77.

232 CICR, *Derecho Internacional Humanitario y terrorismo: respuestas a preguntas clave.* Documento de 1 de enero de 2011. Disponible en el sitio web: www.icrc.org/spa/resources/documents/ faq/ 5yyqg4.htm. Fecha de consulta, junio de 2013.

233 Así lo expresa MARTINEZ ALCAÑIZ quien, en este sentido, afirma, además, que "*los actos terroristas son pluridimensionales, al cometerse tanto en tiempo de paz, como en tiempo de conflicto armado u ocupación bélica, debiéndose distinguirse los unos de los otros*". MARTINEZ ALCAÑIZ, A., *El Derecho Penal Internacional frente a los actos de terror acaecidos durante un conflicto armado.* Revista de Derecho Militar, núm. 102. Julio-Diciembre 2014; pp. 89-128, en particular, p. 100.

> "aquellos comportamientos prohibidos por el DIH, llevados a cabo por una parte beligerante contra la población civil o aquellas personas que han dejado de participar directamente en las hostilidades con la finalidad principal de infundir terror entre las mismas o compeler a la otra parte beligerante para que hagan o dejen de hacer algo, causándose la muerte o lesiones de dichas personas, daños graves en sus bienes esenciales o perjudicar otra serie de valores importantes protegidos por el DIH"[234].

En consecuencia, los obstáculos impuestos por el DIH convencional y consuetudinario deberán ser considerados a la hora de calificar la correspondiente conducta, pues si la parte beligerante o las personas, que han dejado de participar directamente en las hostilidades actúan por cuenta del Estado, o reuniendo las condiciones que se verán más adelante, podrá exigirse responsabilidad internacional al Estado como resultado de su acción u omisión. En cualquier caso, esta específica situación requiere de un estudio más detallado, que se realizara con ocasión del análisis de los requisitos de atribución del hecho ilícito.

2.1.4 El Ciberespionaje.

Existen, por último, determinadas actividades en el ciberespacio, susceptibles de ser encuadradas en distintos ámbitos y que, además, pueden desarrollarse tanto en tiempo de paz como de conflicto armado. Sin embargo, en la mayoría de las ocasiones, éstas quedarán al margen de la conceptuación de ataque armado que ha sido formulada. Es éste el caso de los supuestos del llamado ciberespionaje.

Estas actividades de inteligencia, realizadas a través de medios cibernéticos, ofrecen tanto una perspectiva activa como pasiva. Con esto quiere decirse que, por un lado, habrá que estudiar el marco jurídico, en que deba desarrollarse la obtención de información relativa a terceros Estados, sin incurrir en ilícito, conforme a la legislación interna. Pero, por otra parte, no cabe duda de que, cualquier información, obtenida a través de medios cibernéticos, manifestará

234 Así lo expresa PIGNATELLI Y MECA, F., en cita recogida por MARTINEZ ALCAÑIZ, A., *El Derecho Penal Interna*cional, op. cit; p. 103.

la vulnerabilidad del Estado, que sufre el espionaje, de forma que habrá que atender a las medidas de seguridad, necesarias para evitar la fuga de información, relativa a la Seguridad o Defensa Nacional.

En el ámbito del Derecho interno, como pone de manifiesto LOPEZ ALFRANCA[235], la actividad de inteligencia se halla limitada, esencialmente, por la Constitución, al garantizar la existencia de un Estado de Derecho, con las consiguientes implicaciones normativas que ello conlleva. Es decir, que el lícito uso de los servicios dedicados a la Inteligencia requiere la sujeción de su actuación, entre otras, al respeto a los Derechos Fundamentales consagrados en el Texto Constitucional, así como a la Ley Orgánica 2/2002 de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

En el ámbito del Derecho Internacional, la Convención de Viena sobre Relaciones Diplomáticas de 1961 [236] garantiza la protección, tanto de las comunicaciones, como de los archivos diplomáticos. Esta misma protección es la

235 La regulación de los derechos fundamentales, que pueden verse afectados por las actividades de Inteligencia, así como, las limitaciones que, a estos servicios, son de aplicación en el Derecho interno, son objeto de exhaustivo estudio por parte de LOPEZ ALFRANCA, M. V., *¿Pero quién vigilará a los vigilantes?*.Revista ICADE, núm. 92 (Monográfico dedicado a: Seguridad y Defensa. Reflexiones a la luz de la Estrategia de Seguridad Nacional 2013); mayo-agosto 2014; pp.107-142.

236 En concreto, el articulo 24 de la Convencion, establece que "*Los archivos y documentos de la misión son siempre inviolables, dondequiera que se hallen*" y, por su parte, el articulo 27, que "*El Estado receptor permitirá y protegerá la libre comunicación de la misión para todos los fines oficiales. Para comunicarse con el gobierno y con las demás misiones y consulados del Estado acreditante, dondequiera que se radiquen, la misión podrá emplear todos los medios de comunicación adecuados, entre ellos los correos diplomáticos y los mensajes en clave o en cifra. Sin embargo, únicamente con el consentimiento del Estado receptor podrá la misión instalar y utilizar una emisora de radio. 2. La correspondencia oficial de la misión es inviolable. Por correspondencia oficial se entiende toda correspondencia concerniente a la misión y a sus funciones. 3. La valija diplomática no podrá ser abierta ni retenida. 4. Los bultos que constituyan la valija diplomática deberán ir provistos de signos exteriores visibles indicadores de su carácter y sólo podrán contener documentos diplomáticos u objetos de uso oficial. 5. El correo diplomático, que debe llevar consigo un documento oficial en el que conste su condición de tal y el número de bultos que constituyan la valija, estará protegido, en el desempeño de sus funciones, por el Estado receptor. Gozará de inviolabilidad personal y no podrá ser objeto de ninguna forma de detención o arresto. 6. El Estado acreditante o la misión podrán designar correos diplomáticos ad hoc. En tales casos se aplicarán también las disposiciones del párrafo 5 de este Artículo, pero las inmunidades en él mencionadas dejarán de ser aplicables cuando dicho correo haya entregado al destinatario la valija diplomática que se le haya encomendado. 7. La valija diplomática podrá ser confiada al comandante de una aeronave comercial que haya de aterrizar en un aeropuerto de entrada autorizado. El comandante deberá llevar consigo un documento oficial en el que conste el número de bultos que constituyan la valija, pero no podrá ser considerado como correo diplomático. La misión podrá enviar a uno de sus miembros, a tomar posesión directa y libremente de la valija diplomática de manos del comandante de la aeronave*". Convenion de Viena sobre Relaciones Diplomáticas, de 18 de abril de 1961.

que, a tenor del contenido de la Norma 84 del Manual de Tallin, habrá de garantizarse en el empleo del medio informático[237]. En efecto, con los autores de dicha obra, se puede afirmar que el respeto a la confidencialidad, integridad y disponibilidad de los archivos y comunicaciones diplomáticos exige que las partes en conflicto "*refrain from any action that would interfere with their transmission or reception or impugn their maintenance*[238]". A las tres características tradicionales, se hace necesario añadir una cuarta: la resiliencia[239]. La ciber-resiliencia habrá de entenderse, conforme a lo que ya ha quedado expuesto en el Capítulo precedente, como la capacidad de la organización atacada para prevenir, resistir y reanudar su actividad, una vez producido el ciberataque. En el ámbito del ciber espionaje el elemento de la resiliencia resultará de mayor importancia, pues es el que garantizará la observancia los tres elementos anteriores.

Sin embargo, una vez producida la vulneración del sistema de seguridad, habrá que acudir, en primer lugar, a la regulación interna que, para estas conductas, está prevista en el ámbito penal. En el caso español, no puede obviarse que las conductas relativas a estas actividades, en tiempo de paz, hallarán su respuesta en el artículo 25 del Código Penal Militar que castiga tanto al extranjero como al militar español que incurran en delito de espionaje[240]. En

237 Los autores del Manual de Tallin formulan la Norma 84 cuya redacción ha sido alcanzada en virtud del consenso de todos ellos. Extienden dicha aplicación tanto al conflicto armado internacional como no internacional y recuerdan el fallo de la CJI en relación a la Embajada de EEUU en Irán, que, en el párrafo 24 de su fallo afirmó que: "*[b]y a number of provisions of the Vienna Conventions of 1961 and 1963, Iran was placed under the most categorical obligations, as a receiving State, to take appropriate steps to ensure the protection of the United States Embassy and Consulates, their staffs, their archives, their means of communication and the freedom of movement of the members of their staffs*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p. 192.

238 *Ibidem*; p. 192.

239 Asimismo, el Manual de Tallin entiende que "*Beyond this classic CIA triangle of security, we believe it is important to add another property: resilience. Resilience is what allows a system to endure security threats instead of critically failing*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit; p. 193.

240 El artículo 25 del Código Penal Militar establece: "*El extranjero que, en situación de conflicto armado, se procurare, difundiera, falseare o inutilizare información clasificada como reservada o secreta o de interés militar susceptible de perjudicar a la seguridad o a la defensa nacionales, o de los medios técnicos o sistemas empleados por las Fuerzas Armadas o la Guardia Civil o las industrias de interés militar, o la revelase a potencia extranjera, asociación u organismo internacional, será castigado, como espía, a la pena de diez a veinte años de prisión. El militar español que cometiere este delito será considerado autor de un delito de traición militar y castigado con la pena prevista en el artículo anterior*". Código Penal Militar. Ley Orgánica 14/2015, de 14 de octubre. BOE núm. 247, de 15 de octubre de 2015

conjunción con lo anterior, el CP sanciona idénticas conductas realizadas por cualquier español, es decir, al margen de su condición militar[241].

Por último, podría ocurrir que determinadas actuaciones relativas a ciber espionaje se produjeran, en el marco de un conflicto armado internacional o no internacional. En estos supuestos, podría darse el caso de que los equipos, sistemas o información, perdieran la protección de la que disfrutan, pasando así a convertirse en objetivos militares[242], en el sentido que se expresará al abordar el contenido de la obligación internacional violada y tal y como pone de manifiesto el Manual de Tallin, al afirmar que

> "a State's responsibility for an act of cyber espionage conducted by an organ of the State in cyberspace is not be engaged as a matter of international law unless particular aspects of the espionage violate specific international legal prohibitions (as in the case of cyber espionage involving diplomatic communications)".[243]

3. LAS DISTINTAS CONSECUENCIAS DE LA VIOLACIÓN DE LA OBLIGACIÓN INTERNACIONAL, EN FUNCIÓN DEL CONTEXTO EN QUE SE PRODUZCA EL CIBERATAQUE.

Pues bien, a pesar de que la alerta sobre el elemento cibernético ya se había puesto de manifiesto años antes, tanto en nuestro ámbito interno[244], como

241 Por su parte, el artículo 584 del Código Penal establece: "*El español que, con el propósito de favorecer a una potencia extranjera, asociación u organización internacional, se procure, falsee, inutilice o revele información clasificada como reservada o secreta, susceptible de perjudicar la seguridad nacional o la defensa nacional, será castigado, como traidor, con la pena de prisión de seis a doce año*s". Código Penal. Ley Orgánica 10/1995, de 23 de noviembre. BOE núm. 281, de 24 de noviembre de 1995

242 Esta conclusión es alcanzada por los autores del Manual de Tallin que, en este sentido afirman: "*If diplomatic cyber equipment and communications are misused during an armed conflict, they may, depending on the nature of the misuse, become military objectives since the law of diplomatic relations is not a self-contained normative regime. In such a case, they accordingly lose protection from cyber operations, including cyber attacks*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p.193.

243 Así queda recogido en la Norma 6 del Manual de Tallin. SCHMITT, M.N. (General Editor). Tallin Manual, op.cit.; p. 36.

244 Como recuerda FELIU ORTEGA, en la Revisión Estratégica de la Defensa del año 2003 ya se había puesto de manifiesto que los ciberataques constituyen un riesgo para la seguridad. FELIU ORTEGA, L. *La ciberseguridad y la Ciberdefensa*", El Ciberespacio. Nuevo escenario de confrontación. CESEDEN Monografía, núm. 126, febrero 2012; pp.35-69.

por parte de la doctrina internacionalista[245], los ataques de esta naturaleza sufridos por Estonia y otras Repúblicas bálticas, en los años 2007 y siguientes evidenciaron la fragilidad de determinadas infraestructuras de esos Estados. La virulencia de esos ciberataques, la naturaleza de los objetivos que resultaron atacados, así como la imposibilidad, prácticamente absoluta, de identificar a sus autores y llevarlos ante la justicia, hicieron que la doctrina internacionalista se planteara cuál había de ser la respuesta que, desde el punto de vista jurídico, debería darse a esta nueva forma de amenaza[246].

Estos ataques y otros, de similar índole, además, vuelven a poner de relieve la ambigüedad de su naturaleza y la necesidad de una rápida calificación jurídica. Es decir, como más adelante se verá, al margen del desarrollo de un conflicto armado, puede tenerse constancia de ciberataques que, si bien, no son lanzados en un contexto bélico, sin embargo, si pueden ser detonadores del mismo. Por ello, será necesario tener en cuenta que, en tiempo de paz, puede sufrirse un ciberataque de la virulencia y características de los que han sido descritos en el anterior Capítulo como ataques armados. Sin embargo, en ocasiones, dichos ataques pueden comenzar manifestándose de un modo menos agresivo y, por ende, la evolución de los mismos deberá ser paralela al cambio en su calificación jurídica.

Los ataques sufridos por Estonia, en su día, alcanzaron objetivos que pueden ser considerados infraestructuras críticas, como el teléfono de emergencias médicas y, sin embargo, las lagunas legales, así como otros impedimentos de tipo procedimental, impidieron la exigencia de responsabilidad de sus autores[247].

---

245 De este modo se alertaba sobre la posibilidad del desencadenamiento de la guerra virtual por ARQUILLA, J. y RONFELDT, D. en, *Cyberwar is Coming!. Comparative Strategy*, vol. 12, no. 2, Spring 1993; pp. 141–165.

246 Así puede leerse en la obra citada, del Centro de Excelencia de OTAN, TIKK, E. KASKA, K., VIHUL, L. International Cyberincidents. Legal Considerations, op. cit.; pp. 36-47.

247 En relación al detallado desarrollo de estos hechos, así como de las consecuencias jurídicas de los mismos, la obra publicada por el Centro de Excelencia de OTAN de Estonia, resulta una referencia imprescindible. TIKK, E. KASKA, K., VIHUL, L., International cyber incidents: Legal considerations, op. cit.; pp.14-35.

A partir de ese momento, diversas Organizaciones Internacionales tomaron la iniciativa en el estudio y ofrecimiento de soluciones jurídicas en esta nueva materia. No puede obviarse, en este punto, la labor realizada por la OTAN, cuyos esfuerzos han originado la creación del Centro de Excelencia de Ciberdefensa con sede, precisamente, en Tallin (Estonia) [248].

En definitiva, el interés de la Comunidad Internacional en la neutralización de estas ciberamenazas, desde un punto de vista material, conlleva también, como se ha anticipado, la búsqueda de una oportuna repuesta legal que impida, no sólo la proliferación de este tipo de amenazas, sino también la debilitación del Estado que las sufre.[249]

Como se viene constatando, las distintas manifestaciones de los ataques informáticos exigen un estudio de los mismos, que permita apreciar en qué momento ese ataque supone un acto de agresión, o bien, traspasa el referido "*umbral de violencia*" y, de ese modo, constatar la existencia de un conflicto armado sea éste internacional, en el primer caso o no internacional, en el segundo.

En ambos supuestos, la aplicación del DIH resulta incuestionable. Sin embargo, en este punto, se impone un análisis adicional, acorde con la singular naturaleza del elemento cibernético. Una vez determinada la naturaleza jurídica de los ciberataques, considerados éstos como método de combate, no puede ignorarse el específico contexto en el que estos ataques pueden revelarse. Así, partiendo de la base de que los ataques cibernéticos pueden aparecer tanto en un

248 Los Centros de Excelencia de OTAN consisten, como la propia Organización expone en, "*nationally or multi-nationally funded institutions that train and educate leaders and specialists from NATO member and partner countries, assist in doctrine development, identify lessons learned, improve interoperability, and capabilities and test and validate concepts through experimentation. They offer recognised expertise and experience that is of benefit to the Alliance and support the transformation of NATO, while avoiding the duplication of assets, resources and capabilities already present within the NATO command structure*". Esta definición, así como la estructura, funciones y publicaciones del COE de Estonia, puede ser consultada en su sitio web: https://ccdcoe.org/index.html.

249 Esta conclusión puede alcanzarse examinado el documento de Naciones Unidas A more secure world: *Our shared responsibility*", cuando afirma*: «Every threat to international security today enlarges the risk of other threats. Nuclear proliferation by States increases the availability of the materiel and technology necessary for a terrorist to acquire a nuclear weapon. The ability of non-State actors to traffic in nuclear materiel and technology is aided by ineffective State control of borders and transit through weak States». A more secure world: Our shared responsibility.* Report of the High-level Panel on Threats, Challenges and Change. United Nations 2004; par. 20.

conflicto armado internacional como en uno no internacional habrá, además, que ver si ese ataque constituye la única manifestación de la fuerza presente en ese conflicto o bien, se trata de un método de combate, empleado en concordancia con otros, que podríamos llamar convencionales.

En el primer caso, nos encontraríamos ante lo que puede denominarse ciberguerra y en el segundo ante el desarrollo de operaciones cibernéticas, en el contexto de un conflicto convencional. Por último, podría darse el supuesto en el que el ciberataque constituyera una manifestación del uso de la fuerza que originara un conflicto armado que, también en este caso, pudiera ser internacional o no, y que se pudiera manifestar, bien a través de ciberguerra o como una operación cibernética en un conflicto convencional.

En este estudio será preciso valorar, de nuevo desde una perspectiva teórico-práctica, los criterios de apariencia del ciberataque y el contexto en el que se ha manifestado, en casos ya constatados.

La utilización de las armas basadas en los últimos desarrollos tecnológicos, parece ser la tendencia de los conflictos del siglo XXI y ello permite constatar dos características muy particulares en éstos, como son la globalización y asimetría[250]. Es evidente que el uso de internet facilita, de modo extraordinario, la globalización de los conflictos bélicos, de modo que, el estado de opinión, sobre los mismos, se extiende más allá de las partes implicadas en ellos, dando lugar, incluso, a la posible intervención de terceros. Por otra parte, la asimetría se deriva de la intervención de "*los actores más débiles a tratar de influir sobre la opinión pública del adversario*" [251]. Es decir, en este ámbito, puede decirse que internet ha impulsado un avance, de lo que vino a llamarse "efecto CNN", que definía el impacto que los conflictos tenían en la sociedad civil, a una influencia inmediata que la propia sociedad puede generar a través de la red[252].

250 Así lo expresa PÉREZ NÚÑEZ, P.A., en *La paz y el fin de las narrativas*. Nuevas guerras nuevas paces. Monografias núm. 131. Centro Superior de Estudios de la Defensa Nacional. Septiembre 2012; pp. 17-66, en particular, p. 29.
251 PÉREZ NÚÑEZ, P.A., *La paz y el fin de las narrativas*, op. cit; p. 29.
252 Estas cuestiones son ampliamente consideradas en la obra, *Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción*. En concreto, resulta de especial interés TORRES SORIANO, M. *Guerras youtube. El impacto de las nuevas tecnologías de la información en el*

En estos nuevos conflictos, el elemento cibernético podrá manifestarse, de forma exclusiva, en aquéllos supuestos en que la contienda se libre, únicamente, en el ciberespacio, o bien, podrá aparecer, en combinación con otras operaciones, desarrolladas por métodos y medios de combate, que son los hasta ahora conocidos. Asimismo, podrán darse supuestos en que estos ciberataques, desencadenen por sí mismo, conflictos bélicos tradicionales o cibernéticos.

En todos estos supuestos será imprescindible, nuevamente, atenerse al Derecho Internacional Convencional y Consuetudinario y, partiendo de las definiciones y conceptos que se han examinado, analizar la licitud del uso de internet en los distintos escenarios, como paso previo a la posible exigencia de responsabilidad internacional del Estado que los cometa.

3.1. La ciberguerra.

Aunque la delimitación entre ciberseguridad, ciberdefensa y ciberguerra ha querido trazarse de forma muy clara desde el principio por parte de la doctrina[253], en realidad, la línea que separa estos conceptos, como ha podido comprobarse, es siempre difusa y, a veces, exigua. No obstante, puede aseverarse que nos encontraremos ante un supuesto de ciberguerra en aquellos casos en que el conflicto se desarrolle, exclusivamente, a través de este medio. Tomando la definición de SANCHEZ DE ROJAS, la ciberguerra, es la guerra que "*se produce, total o parcialmente, en la quinta dimensión, la virtual y que implica fundamentalmente las tecnologías de la información y de las comunicaciones*"[254]. Si bien hasta la fecha han sido verificados en la práctica, distintos supuestos de ciberataques y ciberoperaciones, sin embargo, no ocurre lo mismo con la ciberguerra, de la que no se tiene constancia fáctica hasta la fecha. Teniendo en cuenta la experiencia

---

tratamiento mediático de los conflictos armados. Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción. Instituto Español De Estudios Estratégicos. Centro Mixto Universidad De Granada-Mando De Adiestramiento y Doctrina Del Ejército De Tierra. Cuadernos de Estrategia, núm. 148. Agosto 2010; pp. 131 a 157.

253 En este sentido, puede consultarse el capítulo, HATHAWAY, M.E., and KLIMBURG; A. *Preliminary considerations: on national cyber security*. National cyber security framework manual. NATO Cooperative Cyber Defence Centre of Excellence. (Ed., Alexander KLIMBURG). Tallin 2012; pp.1-43.

254 Esta definición es aportada por el autor en su ya mencionado artículo publicado en la Revista Ejército. SANCHEZ DE ROJAS DIAZ, E., *¿Ciber…qué?*, doc.cit; p.141.

hasta ahora sufrida parece evidente que el desarrollo de una ciberguerra no resulta especialmente probable[255].

Sin embargo, ello no obsta al estudio de la misma y, por ende, de sus implicaciones jurídicas, de forma que no resulta ocioso recoger las conclusiones que la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja[256], expresó en el sentido de entender que uno de los desafíos para la aplicación del DIH, en relación a los conflictos armados contemporáneos, estaba constituido por lo que dio en llamarse ciberguerra. El documento resultante de dicha Conferencia puso de relieve que, cualquier medio, conectado a Internet, puede convertirse en un objetivo, susceptible de ser atacado, desde cualquier parte del mundo. Por lo tanto, las redes informáticas de uso militar pueden constituir el objetivo de un ataque informático y, a la vez, un medio para atacar.

Para confirmar la existencia de un conflicto que pudiera calificarse como ciberguerra, habrá que analizar, nuevamente, la definición que el DIH proporciona de conflicto armado. La distinción, derivada del contenido del artículo 3 común a los Convenios de Ginebra de 1949 y, en el caso de los conflictos armados no internacionales, de la definición del artículo 1 del PA II dicta que, desde el punto de vista jurídico, no existe ningún otro tipo de conflicto armado, aunque siempre habrá que tener presente que una situación puede evolucionar de un tipo de conflicto armado a otro, según los acontecimientos que se registren.

En adición a lo anteriormente expuesto, el artículo 2, común a los Convenios de Ginebra de 1949, establece:

> "Aparte de las disposiciones que deben entrar en vigor ya en tiempo de paz, el presente Convenio se aplicará en caso de guerra

255 Algunos autores, incluso, manifiestan su convencimiento de que tal situación nunca llegará a producirse. En este sentido puede consultarse RID, Th., *Cyber War Will Not Take Place*. Journal of Strategic Studies, Vol. 35, núm. 1. Febrero 2012; pp. 5-32.

256 La XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja se celebró en Ginebra, entre noviembre y diciembre de 2011 y los resultados arrojados por la misma pueden ser consultados en el documento CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*. Informe resultante de la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja Comité Internacional de la Cruz Roja. Ginebra, Suiza octubre 2011.

> declarada o de cualquier otro conflicto armado que surja entre dos o varias Altas Partes Contratantes, aunque una de ellas no haya reconocido el estado de guerra.
>
> El Convenio se aplicará también en todos los casos de ocupación total o parcial del territorio de una Alta Parte Contratante, aunque tal ocupación no encuentre resistencia militar".

Un conflicto armado internacional es, por lo tanto, aquel en que se enfrentan las "Altas Partes Contratantes", es decir, aquél en que los Estados sostienen el enfrentamiento. En un conflicto armado internacional, uno o más Estados recurren a la fuerza armada, contra otro Estado, sin que sean trascendentes aquí las razones o la intensidad del enfrentamiento. Las normas pertinentes del DIH son de aplicación, aun cuando no haya hostilidades abiertas y, sin que sea necesaria una declaración de guerra oficial, o un reconocimiento de la situación. De igual modo, resulta irrelevante, a los efectos de la definición que se aborda, la duración del conflicto. El PA I amplía la definición de conflicto armado internacional a aquéllos conflictos armados, en que los pueblos luchan contra la dominación colonial y la ocupación extranjera y contra los regímenes racistas, en el ejercicio del derecho de los pueblos a la libre determinación, es decir, las llamadas guerras de liberación nacional.

Por otra parte, la definición de conflicto armado no internacional se infiere de lo expuesto en el artículo 3, común a los Convenios de Ginebra de 1949 y en el artículo 1 del PA II. En virtud del artículo 3 común dicha definición se aplica a un "*conflicto armado que no sea de índole internacional y que surja en el territorio de una de las Altas Partes Contratantes*". Por lo tanto, en él pueden participar uno o más grupos armados no gubernamentales y podrán darse hostilidades, entre las Fuerzas Armadas gubernamentales y grupos armados, no gubernamentales o entre esos grupos, únicamente.

Desde el punto de vista conceptual, por lo tanto, la asimilación de esta forma de conflicto a la guerra convencional, es posible, tal y como han manifestado los autores del citado Manual de Tallin, que proponen la aplicación del DIH, a los supuestos de ciberguerra, de la misma forma que se aplica a los

conflictos armados hasta ahora conocidos[257]. Esta aplicabilidad se justifica por la asunción del principio que afirma que, el hecho de que una actividad militar no esté concretamente regulada, no significa que pueda desarrollarse sin restricciones, antes bien, los Estados y otras partes, involucradas en un conflicto armado, están obligados a respetar y hacer respetar el DIH.

Esta obligación se extiende a los Estados y otras partes que resultan compelidos, además, a utilizar su influencia para prevenir y poner fin a las infracciones del mismo, así como a abstenerse de alentar la comisión de infracciones, por otras partes.

El respeto y la efectiva aplicación del DIH se revelan esenciales, en el desarrollo y conducción de los conflictos armados, ya se traten éstos de guerras tradicionales entre Estados o de conflictos armados internos, de carácter no internacional.

En el caso de la ciberguerra tampoco puede obviarse la posibilidad de que se produzca como un conflicto no internacional. Un claro ejemplo de ello lo constituyen los ataques sufridos por Bielorrusia. No puede decirse que este supuesto revistiera la entidad suficiente para desencadenar una ciberguerra, pero sí resulta ejemplificador de hasta qué punto, la ciberguerra podría desarrollarse como un conflicto armado no internacional[258].

En ningún caso, por lo tanto, puede entenderse que la ciberguerra quede al margen de la regulación Convencional de estos principios, tal y como se dispone en el artículo 1, común a los Convenios de Ginebra y al PA I. Esta declaración no puede ser obviada por cuanto cumple la función adicional de contribuir a la constitución de un orden público internacional. En la actualidad,

257 En este sentido se expresa el Manual en su conjunto y más específicamente en su Norma 20. SCHMITT, M.N. (General Editor).Tallin Manual, op. cit.; pp. 68-70.

258 El Centro de Excelencia de Ciberdefensa de OTAN examinó este supuesto como uno de los que las Repúblicas bálticas sufrieron a finales de la década pasada. En este caso se dio la circunstancia de que la población civil de Bielorrusia fue objeto de ataques informáticos procedentes, con toda seguridad, de agentes de su propio Estado. Los mismos se produjeron en un contexto en el que la población, contraria a la actuación del Gobierno, acusaba a éste de haber desatendido a las víctimas de la catástrofe de Chernóbil. En tales circunstancias, una emblemática emisora de radio (Radio Free-Radio Liberty), lideró la emisión de los mensajes de protesta, siendo, como consecuencia, atacada su página web hasta el punto de dejarla inoperativa. TIKK, E. KASKA, K., VIHUL, L,. International Cyberincidents, op. cit.; pp. 36-47.

este orden público puede verse amenazado por una ciberguerra de la misma forma que se ve alterado diariamente por la conducción de conflictos que podríamos calificar de convencionales.

Tampoco puede olvidarse, por otra parte, el compromiso y la responsabilidad de los Estados que son Parte en los principales Tratados Humanitarios, por cuanto quedan obligados a tomar las medidas imprescindibles para garantizar el respeto al DIH, incluso, por parte de un tercer Estado, en particular si este Estado es una parte en un conflicto armado[259].

Asumida, por tanto, la posibilidad de que nos encontremos ante una ciberguerra y dando por sentado que, a la misma le será de aplicación el DIH, es preciso traer a colación, de nuevo, la definición del término «ataque». Si en el Capitulo precedente, se realizaba un análisis de este concepto, a la luz del Derecho Internacional, en este momento, resulta necesario ese mismo análisis, en virtud de lo dispuesto en la específica rama del DIH para, de este modo valorar si dicho concepto resulta adecuado a este nuevo contexto bélico.

El PA I y el DIH consuetudinario contienen una definición específica del término, en cierto modo divergente de la ofrecida por otras ramas del Derecho. En virtud del artículo 49.1 del PA I, se entiende por «ataques» los actos de violencia contra el adversario, sean ofensivos o defensivos. La expresión «actos de violencia» ha sido entendida como aquélla que denota fuerza física[260]. Sobre la base de esta interpretación, las operaciones cibernéticas que causan un daño físico a las personas u objetos han de ser calificadas como «actos de violencia», es decir, ataques en el sentido del DIH[261].

---

259 Así queda reflejado por CÁCERES BRUN, J. *El sistema de eficacia del Derecho Internacional Humanitario*. Derecho Internacional Humanitario. (Coord. Rodríguez-Villasante y Prieto, J.L.). Cruz Roja Española. Centro de Estudios de Derecho Internacional Humanitario. Tirant lo Blanch. Valencia 2002; pp. 623-644, en particular; p. 624.

260 En este sentido, es interesante la reflexión aportada por HUGHES, R., en *Towards a Global Regime for Cyber Warfare*, en CZOSSECK, CH. and GEERS, K. (Eds.), The Virtual Battlefield: Perspectives on Cyber Warfare.IOSS Press. Amsterdam. 2009; pp.106-117.

261 Expresamente, el Artículo 49, al definir los ataques, establece: «*1. Se entiende por ataques los actos de violencia contra el adversario, sean ofensivos o defensivos. 2. Las disposiciones del presente Protocolo respecto a los ataques serán aplicables a todos los ataques en cualquier territorio donde se realicen, inclusive en el territorio nacional que pertenezca a una Parte en conflicto, pero que se halle bajo el control de una Parte adversa. 3. Las disposiciones de la presente Sección se aplicarán a cualquier operación de guerra terrestre, naval o aérea que pueda afectar en tierra a la población civil, a las personas civiles y a los*

En conexión con lo anterior, los ataques que tengan lugar en la conducción de la ciberguerra se verán sujetos, al menos, a las mismas restricciones y obligaciones que se imponen, en la conducción de las hostilidades, en los conflictos, hasta ahora conocidos. Consecuentemente, estos ataques sólo podrán dirigirse contra los objetivos militares, cuando exista una necesidad militar, con observancia del principio de proporcionalidad, sin hacer uso de perfidia y respetando la neutralidad de terceros, como se verá con más detalle en el epígrafe correspondiente.

Por lo tanto, la exigencia de responsabilidad en virtud del DIH, en el supuesto de que se dirigiera una operación que contraviniera dichos principios y limitaciones en la conducción de hostilidades, en el contexto de una ciberguerra, habrá de realizarse de igual modo que lo hubiera sido en el caso de que ese objetivo civil se hubiera atacado en una guerra convencional.

Sin perjuicio de que, todas las anteriores normas relativas a la conducción de hostilidades sean de preceptiva observancia y, por ello, serán objeto de análisis pormenorizado, la prohibición de los ataques indiscriminados, constituye una tarea desafiante, en lo que a la ciberguerra concierne. La interconectividad de redes civiles y militares y la posibilidad de actuar, desde cualquier parte del mundo, contra la red informática u objetivo, presentes en otro Estado, distinto del que envía el ataque, hace que esta norma cobre un especial protagonismo. No cabe duda de que una de las ventajas que presentan los ataques informáticos es la posibilidad de elegir, con precisión, el lugar, momento de inicio, de finalización del ataque y efectos a conseguir. Por ello y, también, porque los ataques indiscriminados se presentan como sumamente sencillos en su lanzamiento, conviene tener presente la absoluta aplicabilidad de esta norma. Como

---

bienes de carácter civil. Se aplicarán también a todos los ataques desde el mar o desde el aire contra objetivos en tierra, pero no afectarán de otro modo a las normas de derecho internacional aplicables en los conflictos armados en el mar o en el aire. 4. Las disposiciones de la presente Sección completan las normas relativas a la protección humanitaria contenidas en el IV Convenio, particularmente en su Título II, y en los demás acuerdos internacionales que obliguen a las Altas Partes contratantes, así como las otras normas de derecho internacional que se refieren a la protección de las personas civiles y de los bienes de carácter civil contra los efectos de las hostilidades en tierra, en el mar o en el aire».

acertadamente señala SCHMITT, ello ha de ir acompañado de una creciente necesidad de interpretación del DIH[262].

Sin embargo, si retomamos la definición de ataque, anteriormente citada, parece conveniente señalar que la ausencia de destrucción física no debería impedir la aplicación del DIH. Habrá que tener presente que, en caso de ciberconflicto, el ataque lanzado desde una red militar, contra una red civil, de forma indiscriminada, no debería impedir la aplicación del DIH por más que, *a priori*, no cause daños físicos. Si con ese ataque se pone en peligro, por ejemplo, una vía de comunicación de emergencias sanitarias para la población civil, la posibilidad de que se sufran daños físicos, por parte de la misma, no resulta remota, aunque no sea ése el primer resultado. Consecuencia inevitable de la afirmación anterior, será la exigencia de responsabilidad a quien, encontrándose al Mando de una operación, hubiera ordenado ese ataque, o debiera haber conocido que se estaba produciendo por parte de un subordinado[263].

De igual forma, como también se vera pormenorizadamente, al atender al contenido de la norma de DIH violada, el DIH prohíbe los ataques desproporcionados. En este sentido, se plantea la cuestión de si, en la práctica, resulta posible anticipar, totalmente, las consecuencias o los efectos secundarios

---

262 SCHMITT, al respecto, entiende que "*There is no doubt that precision operations have opened up new possibilities for avoiding the harm to civilians and their property that is the inevitable result of armed conflict. In that sense, advances in precision represent a positive trend. Further, as weaponry becomes more precise, interpretation of international humanitarian law is becoming increasingly demanding for an attacker. So long as such interpretations do not depart from the law or ignore the realities of military necessity, this too is to be welcomed. However, when the allure of precision creates exaggerated expectations of its possibilities such that those beyond the battlefield impose unreasonable demands on the military or postulate norms that go beyond treaty or custom, international humanitarian law is weakened Lex ferenda must be clearly distinguished from lex lata. Moreover, to be respected, international humanitarian law must continue to rationally balance humanitarian concerns with military necessity. The balancing may shift along with developments in the nature of warfare, but must remain at the heart of international humanitarian law. Finally, the international humanitarian law community must be sensitive to the fact that when precision capabilities are possessed unequally on the battlefield, the resulting asymmetry may lead the disadvantaged side to resort to tactics that violate the most basic principles of international humanitarian law. This is not to suggest that high-tech forces should abandon their precision technologies to make war more humane. Obviously, any such suggestion is absurd. Rather, it is a call for the community to redouble its efforts to safeguard the principles of international humanitarian law in the face of the likelihood that others will seek to justify their abandonment*." SCHMITT, M. N. *Perfidy and protected status. Precision attack and international humanitarian law*. International Review of the Red Cross. Vol. 87. Number 859 September 2005; pp.445-466, en particular; p. 466.

263 Así se expresan DE TOMÁS MORALES, S. y VELÁZQUEZ ORTIZ, A.P., en *La responsabilidad del Mando en la conducción de las operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz*, op. cit.; pp.117-149.

que un ataque, dirigido contra un objetivo militar legítimo, pueda tener en la población y bienes civiles.

Respetar los principios de distinción y proporcionalidad significa, inevitablemente, tomar algunas precauciones en la conducción del ataque, concretamente las contempladas en el artículo 57 del PA I. Esto incluye la obligación de seleccionar los medios y métodos de ataque, que permitan evitar y, en cualquier caso, reducir al mínimo, las víctimas y daños civiles incidentales. Como ya se ha mencionado, precisamente será en la ciberguerra donde resulte más factible el cumplimiento de esta norma, por cuanto la propia naturaleza del conflicto y del arma, lo permitirán.

Por último, el PA I exige tomar las precauciones necesarias para garantizar que las dos normas anteriores sean respetadas, en particular la obligación de reducir al mínimo los daños civiles incidentales y la obligación de abstenerse de decidir ataques que serían excesivos en relación con la ventaja militar concreta y directa que se espera obtener[264].

264 Las precauciones que establece el artículo 57 del Protocolo Adicional I son las siguientes: "*1. Las operaciones militares se realizarán con un cuidado constante de preservar a la población civil, a las personas civiles y a los bienes de carácter civil. 2. Respecto a los ataques, se tomarán las siguientes precauciones: a) quienes preparen o decidan un ataque deberán: i) hacer todo lo que sea factible para verificar que los objetivos que se proyecta atacar no son personas civiles ni bienes de carácter civil, ni gozan de protección especial, sino que se trata de objetivos militares en el sentido del párrafo 2 del artículo 52 y que las disposiciones del presente Protocolo no prohíben atacarlos; ii) tomar todas las precauciones factibles en la elección de los medios y métodos de ataque para evitar o, al menos, reducir todo lo posible el número de muertos y de heridos que pudieran causar incidentalmente entre la población civil, así como los daños a los bienes de carácter civil; iii) abstenerse de decidir un ataque cuando sea de prever que causará incidentalmente muertos o heridos en la población civil, daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista; b) un ataque será suspendido o anulado si se advierte que el objetivo no es militar o que goza de protección especial, o que es de prever que el ataque causará incidentalmente muertos o heridos entre la población civil, daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista; c) se dará aviso con la debida antelación y por medios eficaces de cualquier ataque que pueda afectar a la población civil, salvo que las circunstancias lo impidan. 3. Cuando se pueda elegir entre varios objetivos militares para obtener una ventaja militar equivalente, se optará por el objetivo cuyo ataque, según sea de prever, presente menos peligro para las personas civiles y los bienes de carácter civil. 4. En las operaciones militares en el mar o en el aire, cada Parte en conflicto deberá adoptar, de conformidad con los derechos y deberes que le corresponden en virtud de las normas de derecho internacional aplicables en los conflictos armados, todas las precauciones razonables para evitar pérdidas de vidas en la población civil y daños a bienes de carácter civil. 5. Ninguna de las disposiciones de este artículo podrá interpretarse en el sentido de autorizar ataque alguno contra la población civil, las personas civiles o los bienes de carácter civil*".

3.2. Operaciones cibernéticas que se desarrollan en el transcurso de un conflicto convencional.

La naturaleza de los conflictos actuales conlleva que, cada vez con más frecuencia, las armas cibernéticas se utilicen en combinación con operaciones cinéticas tradicionales. En este caso, la existencia de un conflicto armado es indudable de forma que la aplicación del DIH resulta, igualmente, inexcusable.

Inicialmente, las operaciones cibernéticas fueron definidas como aquéllas que consisten en operaciones realizadas contra un ordenador o mediante un ordenador o un sistema informático, utilizando para ello el flujo de datos[265]. De la amplitud de esta definición, pueden inferirse una serie de consecuencias que manifiestan la complejidad en la regulación de este nuevo método de guerra. Si por operación cibernética, se entiende cualquier operación realizada contra un ordenador, habrá que tener en cuenta que, a diferencia de otro tipo de armamento, éste puede hallarse en manos casi de cualquier individuo, por lo que resultará especialmente relevante la actuación de dicho individuo a la hora de atribuirle la autoría de unos hechos por los que, eventualmente, sea exigible la responsabilidad del Estado.

La segunda parte de la definición, que entiende por operación cibernética la que se realice mediante un ordenador o sistema informático, exige que se excluyan determinadas actuaciones que, pudiendo ser consideradas ciberataques, sin embargo, no revisten la entidad de operaciones cibernéticas. Probablemente, radique, aquí, una de las mayores dificultades conceptuales, en esta materia.

Hasta el momento, la distinción entre ambos conceptos, únicamente ha podido realizarse con claridad, atendiendo al contexto en que se han producido. Uno de los ejemplos en relación a las ciberoperaciones que puede traerse a colación es la sufrida por Georgia en el año 2008. Es incuestionable que esta operación cibernética fue lanzada en un contexto bélico, por cuanto Georgia se hallaba en una situación de guerra, librada por medios que podemos llamar

265 Informe resultante de la XXXI Conferencia Internacional de la Cruz Roja, doc. cit; p.41.

convencionales, con Rusia como consecuencia de la contienda relativa a la región de Osetia[266].

En este contexto, las operaciones militares en el ciberespacio, también llamadas *computer network operations* (en adelante, CNO) incluyen tanto las acciones, de naturaleza defensiva, como de explotación de las capacidades de los posibles adversarios y de respuesta. La doctrina indica que las capacidades de las CNO se componen de:

-*Computer network defense* (CND) que incluye las medidas adoptadas a través del uso de redes de ordenadores para proteger, controlar, analizar, detectar y responder a la actividad no autorizada en los sistemas de información y comunicaciones. Las acciones c*omputer network defense* no sólo buscan proteger los sistemas de un adversario externo, sino también de su explotación desde dentro de la propia organización,

-*Computer network exploitation* (CNE), que incluye las capacidades de compilación de inteligencia llevadas a cabo a través del uso de redes de computadoras para recopilar datos de los sistemas de información y comunicaciones del posible adversario y

-*Computer network attack* (CNA), que se compone de las medidas adoptadas a través del uso de las redes informáticas para interrumpir, negar, degradar o destruir la información manejada por los sistemas de información y comunicaciones (del posible adversario), o los propios sistemas de información y comunicaciones[267].

Como consecuencia de esta posibilidad de conducir ciberoperaciones, en el contexto de conflictos armados, que no son catalogados como ciberguerra, ha de resaltarse la preocupación que, desde una perspectiva humanitaria, supone el uso este tipo de medios. A través de ellos, resultará posible la manipulación de sistemas de tráfico aéreo, oleoductos, centrales nucleares y todo tipo de

266 En este caso, entre otros efectos, se produjo la imposibilidad de establecer comunicaciones por parte del Ejército de Georgia, como consecuencia de un ataque cibernético, no ofrece duda sobre la categoría de la operación. El Centro de Excelencia de OTAN en el estudio sobre este supuesto afirma que todos los datos apuntan a que la ciberoperación fue lanzada por el Ejército ruso. TIKK, E. KASKA, K., VIHUL, L. International Cyberincidents, op. cit.; pp.66-89.
267 AA.VV. Estrategia de la información y seguridad en el ciberespacio, op. cit.; pp 17-19.

infraestructuras críticas del enemigo. Por ello conviene recordar la obligatoriedad de las normas, ya apuntadas en el apartado anterior. Esa exigencia no viene delimitada, exclusivamente, por la posibilidad material de su aplicación, sino, ante todo, por las devastadoras consecuencias que, en la población civil, podría tener obviarla.

Una de las dificultades que se ha puesto de manifiesto, a la hora de determinar la aplicación del DIH a las operaciones cibernéticas, ha sido la imposibilidad, en la mayoría de las ocasiones, de rastrear la autoría de las mismas, habida cuenta el anonimato que garantiza el ciberespacio[268]. El sistema de exigencia de responsabilidad, articulado por el DIH y ratificado por la práctica consuetudinaria, demanda la atribución de una actividad, bien a un Estado, bien a un individuo que actúe como Agente de aquél y, en consecuencia, el desconocimiento de dicha autoría, complica la labor de la atribución de una conducta. De cualquier modo, siempre habrá que tener presente que la dificultad de indagación de la autoría, en nada puede mermar la determinación en la aplicación del DIH. En todo caso, corresponderá a los Estados, la implantación de medios técnicos que permitan el rastreo de dicha autoría y, en ocasiones, de medidas legales internas que, en el ámbito procesal, faciliten dicha actuación.

Si bien es cierto que, los ataques sufridos por Estonia no pueden categorizarse como una ciberoperación, puesto que ningún conflicto bélico se estaba desarrollando, sí sirven para revelar la dificultad de la indagación de la autoría, correspondiente atribución de la misma y la correlativa exigencia de responsabilidad[269].

---

268 Informe resultante de la XXXI Conferencia Internacional de la Cruz Roja, doc. cit; p.42.

269 En Abril de 2007, Estonia asistió a una serie de manifestaciones callejeras promovidas por grupos de jóvenes de origen ruso. Estas manifestaciones constituían una forma de protesta frente a la decisión del Gobierno de Estonia de cambiar el emplazamiento de una estatua conmemorativa de la victoria soviética frente al Ejército nazi que había permanecido en el centro de Tallin durante décadas, sin que en torno a la misma se hubiesen producido incidentes. A las protestas callejeras se unió una fuerte oposición del Gobierno ruso que, a través de la prensa, realizó una serie de manifestaciones acusando a Estonia de pretender inventar la historia y de glorificar el régimen nazi. Ello conllevó otra oleada de violencia callejera. Los ciberataques comenzaron de modo paralelo a los altercados callejeros y continuaron variando de intensidad hasta el final del mes de mayo. Pueden diferenciarse, no obstante, dos fases de diferente intensidad, una primera que se ha considerado espontánea o emocional, sin una gran organización y consecuencia directa de lo que estaba ocurriendo en las calles de Tallin, y una

Las operaciones cibernéticas pueden tener muy distintos objetivos y manifestaciones. De este modo, es posible destruir, alterar o interrumpir el funcionamiento de diversos objetivos como industrias, infraestructuras, telecomunicaciones, o sistemas financieros, a través del uso malintencionado de la red. El interés del CICR, por lo tanto, se suscita ante las preocupaciones que estas operaciones y sus consecuencias pudieran tener desde una perspectiva humanitaria[270]. Una catástrofe de tal índole podría darse, por ejemplo, si se manipularan los sistemas de tráfico aéreo, los sistemas de oleoductos o las centrales nucleares de un enemigo, si se interfirieran los sistemas informáticos de apoyo.

El hecho de que la actividad cibernética, con fines bélicos, no esté concretamente regulada, no significa que puedan utilizarse, sin restricciones los métodos y medios de guerra que incluyen esta tecnología, sino que éstos, se hallan sujetos a las normas del DIH, como cualquier otra nueva arma o sistema vector empleado hasta la fecha, cuando se utiliza en un conflicto armado por una Parte en ese conflicto o en su nombre. Así, si una operación cibernética fuera utilizada contra un Estado enemigo en un conflicto armado para causar daño, por ejemplo, mediante la manipulación de un sistema de control del tráfico aéreo, difícilmente podría negarse que ese ataque es, de hecho, un medio de guerra y está sometido a las prohibiciones de conformidad con el DIH. Además, hay que recordar nuevamente, el contenido del artículo 36 del PA I, que impone que cuando un Estado Parte estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o, por cualquier otra norma de Derecho Iinternacional, aplicable a ese Estado Parte.

---

segunda con un gran nivel de organización y coordinación y de carácter más intenso. TIKK, E. KASKA, K., VIHUL, L., International Cyberincidents, op. cit.; pp.15-24.

270 Asi se manifiesta la experta jurídica del CICR, Cordula DROEGE que define las "*operaciones cibernéticas*" como las "*operaciones realizadas contra un ordenador, o mediante un ordenador o un sistema informático, utilizando para ello el flujo de datos*". DROEGE, C., No hay lagunas jurídicas en el ciberespacio, doc, cit.

Como consecuencia de los planteamientos anteriores, se ha propuesto la creación de las llamadas "cibercélulas", como herramientas eficaces para el aseguramiento en el ámbito cibernético de la Seguridad y la Defensa[271].

Las dificultades, pues, a la hora de aplicar el DIH, no se manifiestan tanto en un plano teórico, como en el ámbito práctico. En los casos ya citados de los ciberataques que se produjeron en Estonia y Georgia, la dificultad radicó, principalmente, en la imposibilidad de probar que los mismos provenían o contaban con el apoyo expreso de un Estado[272]. En ambos supuestos y, en tantos otros en los que se dieran idénticas circunstancias (como el también señalado de los ataques cibernéticos de Corea del Norte contra la empresa Sony) se estaría, además, ante la dificultad de exigir responsabilidad internacional al Estado, como consecuencia de las constatadas dificultades de atribución de la conducta al mismo. No obstante, esta cuestión será objeto de atención en el Capítulo posterior.

3.3. El ciberataque como factor potenciador de un conflicto armado.

En último lugar, los ataques informáticos pueden ser calificados como meros ciberataques, cuando éstos no se producen en el entorno de ningún contexto bélico. Por su número y frecuencia son éstos los de mayor importancia y

---

271 "*Las cibercélulas estarían compuestas por equipos operacionales y tácticos actuando bajo el control de un mando estratégico cibernético y requieren que antes exista un conjunto de capacidades de ciberseguridad y ciberdefensa tradicionales ya maduras: una infraestructura TIC moderna, un conjunto de capacidades cibernéticas y un personal experimentado y habituado a operar en este entorno. A partir de ahí, las cibercélulas podrían conducir operaciones cibernéticas de naturaleza defensiva y ofensiva, apoyarían la evaluación y mejora de las capacidades nacionales, multinacionales o aliadas, permitirían experimentar con nuevos conceptos operativos o adiestrar al personal destinado en esta organización. Su implementación puede mejorar sensiblemente la capacidad cibernética defensiva y ofensiva de una nación, contribuyendo así al control del ciberespacio y la creación de una ciberfuerza nacional moderna, efectiva y completamente interoperable con las ciberfuerzas aliadas. En el caso especifico de España, y al igual que el resto de sus aliados, los esfuerzos deberán concentrarse en madurar las capacidades cibernéticas de sus Fuerzas y Cuerpos de Seguridad y de sus Fuerzas Armadas a corto y medio plazo como paso previo a una implantación efectiva de una capacidad avanzada como son las cibercélulas. Sin embargo, y al igual que ya hacen los aliados, debería ir sopesando la conveniencia de implantarlas para que las capacidades cibernéticas en desarrollo puedan pasar a ser operativas a la mayor brevedad*". REAL INSTITUTO ELCANO, *Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales*, doc. cit;

272 Así se pone de manifiesto en la obra publicada por OTAN en relación al estudio de estos incidentes, donde puede leerse: "*In neither the Georgia 2008 case nor in the Estonia 2007 case preceding it has it been possible to prove support by any certain state behind the cyber attacks. In conclusion, it is highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks – the objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect.*" TIKK, E., KASKA K., RÜNNIMERI, K., KERT, M., TALIHÄRM, A. M., VIHUL, L. Cyber Attacks Against Georgia: Legal Lessons Identified, op. cit.; p.23.

por su desdibujada naturaleza, los que más problemas ofrecen a la hora de proceder a su calificación jurídica.

El cumplimiento de las normas establecidas en el DIH, puede resultar evidente cuando se examinan supuestos en los que el elemento cibernético constituye, bien una modalidad de conflicto, bien un medio de combate que puede ser utilizado en combinación de otros en un contexto, igualmente bélico.

Sin embargo, conviene recordar que los ataques cibernéticos más representativos, no han producido en este tipo de situaciones. Es el caso, por ejemplo, de los ciberataques de los que fueron objeto Estonia o Lituania en los años 2007 y 2008. Como consecuencia de los mismos, determinados servicios, tanto naturaleza pública como privada, se vieron alterados durante varios días. Asimismo, los ciberatacantes impidieron el funcionamiento de algunas de las entidades bancarias y dejaron, a estos Estados, sin posibilidad de ofrecer información al exterior, por cuanto, también, perturbaron el funcionamiento de diversos medios de comunicación. En todos ellos, el contexto bélico era inexistente, por lo que no pueden valorarse como supuestos de ciberguerra ni de ciberoperaciones y, en principio, pudiera parecer improcedente el planteamiento de la aplicación del DIH[273].

273 En Junio de 2008, el Parlamento de Lituania resolvió modificar la Ley de Reunión, reguladora, asimismo, de la libertad de expresión y de asamblea. De conformidad con esta modificación, quedó prohibida la exhibición pública de himnos y símbolos, tanto nazis como soviéticos. Las protestas que se sucedieron, una vez sancionada la reforma. La Federación Rusa expresó su descontento con la decisión tomada por el Parlamento de Lituania, a través de manifestaciones, tanto de la Presidencia del Gobierno como de su Parlamento. Asimismo, otros países afines a los intereses rusos se pronunciaron de manera similar. Así, el presidente ruso Medvedev y el Presidente de Bielorrusia, conjuntamente, denunciaron la política de Lituania, declarando que decisiones como la que se había tomado, constituían una aproximación politizada a la historia y condenaron lo que estos dirigentes calificaban de "intento de reescribir la historia". En el Parlamento Ruso, se aprobó por unanimidad una declaración que criticaba duramente la decisión lituana, a la que se acusaba de estar insultando la memoria de los soldados soviéticos de la Segunda Guerra Mundial, y su lucha contra los nazis. Posteriormente, el partido Comunista celebró una manifestación frente a la embajada lituana en Moscú. Durante el espacio temporal en el que se produjo la modificación normativa, un gran número de páginas web fueron alteradas, cambiando significativamente su contenido. Unas trescientas websites vieron vulnerada su apariencia habitual y, en lugar de sus contenidos, ofrecieron imágenes pro soviéticas y símbolos comunistas, así como slogans contrarios a Lituania. El mayor número de ciberataques se produjo el 29 de Junio de 2008 y en el mayor pico de actividad se llegaron a registrar ataques a trescientas páginas web simultáneamente. Aunque no fue el único medio de ataque, la mayoría de éstos consistieron en esa alteración de contenido. Las páginas web saboteadas aparecían, entonces, con símbolos comunistas o bien sobre un fondo con la bandera roja. Las páginas incluían mensajes en

La misma reflexión puede hacerse en relación al lanzamiento del virus Stuxnet, contra las centrales nucleares de Irán, en el año 2010[274]. En este caso, a través de la introducción de este virus, la amenaza de guerra nuclear por parte de Irán quedó materialmente anulada al interferir en el desarrollo de su tecnología nuclear[275].

Es indudable que los resultados, que pueden lograrse, a través de un ciberataque, pueden llegar a ser seriamente destructivos. Desde el momento en que, a través de un ataque informático, pueda interferirse, por ejemplo, en el sistema de Defensa Nacional de un Estado, no cabe duda de que, la potencial capacidad de causar daños, a través de un ataque informático es, cuando menos igual, que la de un arma convencional. En una hipotética situación, como la señalada, los efectos, que pudieran producirse, resultarían absolutamente

---

ruso, en contra de Lituania. La embajada de Lituania en los Estados Unidos, informó de que los ataques se habían producido por medios que habían originado una interrupción brusca del servicio, durante la que se había utilizado software PHP. Según iDefense (compañía de seguridad americana), los saboteadores también utilizaron foros de internet y lanzaron correo electrónico *spam*, con objeto de difundir un manifiesto llamado "Hakers Unidos contra las Amenazas Externas hacia Rusia". Su ánimo no era otro que instigar la difusión de ataques similares a otros países, tales como Ucrania, el resto de las Repúblicas Bálticas y, según sus autores, a aquéllos países occidentales que habían alentado y apoyado la expansión de OTAN en el Este de Europa. Estos ciberataques han sido examinados con detalle por parte del Centro de Excelencia de Ciberdefensa de OTAN, entre otras, en la publicación TIKK, E. KASKA, K., VIHUL, L., International Cyberincidents, op. cit. ; pp. 50-57.

274 El virus Stuxnet ha sido definido por algunos autores como: "…*start of a new era in the arms-race in cyber security. First time in history, a targeted cyber attack was discovered that aimed at physically destroying part of the critical infrastructure of a state*". Así se expresan BENCSATH B., et al., en el artículo *The Cousins of Stuxnet: Duqu, Flame, and Gauss*, op. cit.: "*Like other computer worms, Stuxnet spread indiscriminately from one vulnerable computer to the next. What set it apart from the thousands of other worms that went before it is that it was designed to unleash its payload only when it entered an industrial control system (ICS) matching the characteristics of Iran's nuclear enrichment facility at Natanz. And when it did, it tampered with the code of theprogrammable logic controller (PLC) used to control the centrifuges at Natanz, ultimately destroying about a thousand centrifuges and disrupting Iran's nuclear program. No previously reported worm had done anything like that before, either in terms of precision targeting or causing physical damage through ICS manipulation*". También al respecto, puede consultarse DENNING, D. E. *Stuxnet: What Has Changed?*, op. cit. El Manual de Tallin, por su parte define Stuxnet como "*A computer worm that was designed to target software and equipmentcomprising Siemens Corporation developed Supervisory Control and Data Acquisition(SCADA) systems. The payload of the Stuxnet malware included a programmable logiccontroller rootkit. Stuxnet came to light after it was discovered that it had been used totarget Iranian facilities at which Siemens SCADA systems are used to control centrifuges involved in the enrichment of uranium*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p. 214.

275 Al respecto, véase GÓMEZ DE ÁGREDA, A., *El ciberespacio como escenario del conflicto. Identificación de las amenazas*, op. cit.; pp. 202-203 y también, JOYANES AGUILAR, L., Introducción. Estado del arte de la ciberseguridad. C*iberseguridad. retos y amenazas a la seguridad nacional en el ciberespacio*. Instituto Español de Estudios Estratégicos Instituto Universitario «General GUTIÉRREZ Mellado». Cuadernos de Estrategia, núm. 149. Diciembre 2010; pp. 13-46.

demoledores, incluso, en tiempo de paz y, podrían originar el desencadenamiento de hostilidades.

Por ello, parece conveniente reflexionar sobre una eventual aplicación del DIH, a supuestos semejantes, que puedan darse en el futuro. Esta reflexión se justifica desde el momento en que surge la duda de si podría calificarse de conflicto armado, en el sentido de los Convenios de Ginebra y de otros tratados de DIH, aquél en el que los primeros o los únicos actos «hostiles» se perpetran por medio de una operación cibernética.

La aplicación del DIH dependerá de la fase, en la que el conflicto se encuentre, en función de la denominada escalada de la violencia, es decir, las fases a través de las que discurre un conflicto, desde el momento previo a su existencia hasta el restablecimiento de la paz.[276] La diferencia entre un conflicto armado, en el sentido del artículo 3 común a los Convenios de Ginebra y, otras formas menos graves de violencia, vendrá dada, asimismo, por el llamado umbral de enfrentamiento[277]. Para determinar cuál haya de ser éste han sido tradicionalmente utilizados dos criterios: por un lado, se considera que las hostilidades deben alcanzar un nivel mínimo de intensidad y, por otro, que los grupos no gubernamentales, que participan en el conflicto, deben ser considerados "*partes en el conflicto*", en el sentido de que disponen de Fuerzas Armadas organizadas. Esto significa, por ejemplo, que estas fuerzas constituyan una colectividad armada y cuenten con un líder responsable[278].

A la luz de ambos criterios, resulta evidente que ninguno de los mencionados ataques sufridos por las repúblicas bálticas, rebasó ese umbral de violencia, de forma que puede afirmarse que, los disturbios ocasionados por

276 Estas fases son la violencia interna, el conflicto de carácter no internacional, las guerras de liberación nacional, el conflicto internacional y el conflicto internacionalizado. Así lo recoge GUISÁNDEZ GÓMEZ, J. GUISÁNDEZ GÓMEZ, J. *La protección de las víctimas en los conflictos de carácter no internacional*. Derecho Internacional Humanitario. (Coord. Rodríguez-Villasante y Prieto, J.L.). Cruz Roja Española. Centro de Estudios de Derecho Internacional Humanitario. Tirant lo Blanch. Valencia 2002; pp. 433-452, en particular; p.435.

277Así se expresa el documento elaborado por la XXVII Mesa Redonda sobre problemas actuales del DIH, CICR, *Derecho Internacional Humanitario y otros regímenes jurídicos. Interacción en las situaciones de violencia,* doc. cit.; p.3.

278 Al respecto, puede consultarse GUISANDEZ GÓMEZ, J. *La protección de las víctimas en los conflictos*, op. cit.; p.443.

dichos ataques, aun afectando, claramente, a la vida cotidiana de los habitantes de los mencionados países, no pueden calificarse como conflicto armado.

En consecuencia y, puesto que la existencia de un conflicto armado constituye una condición, indispensable, para la aplicación del DIH, la delimitación de las situaciones de violencia, que pudieran entrar en esta calificación, reviste un carácter fundamental, de modo que habrá supuestos en los que, habiéndose producido ciertos daños, no entrarán en dicha calificación.

No obstante, tal labor encuentra el serio obstáculo de que en ningún instrumento convencional puede hallarse la citada definición, al menos, con la precisión que este novedoso ámbito requiere.

4. ORIGEN DE LA VIOLACIÓN.

Como se viene afirmando, la calificación de un hecho como ilícito internacional, en modo alguno depende del origen o fuente de la obligación violada, de forma que los artículos relativos a la responsabilidad internacional del Estado, "*se aplican a todas las obligaciones de los Estados sea cual fuere su origen*" [279] y así, "*tan ilícito es un acto contrario a una obligación de origen consuetudinario como uno que contradiga un compromiso basado en un tratado o en una fuente de otro tipo*"[280].

A pesar de que el reconocimiento al origen consuetudinario de la obligación internacional es antiguo, su mayor reconocimiento puede verse en la sentencia del CIJ de 27 de junio de 1986 sobre las actividades militares y paramilitares en y contra Nicaragua[281].

279 Así se recoge en el Comentario 3) al artículo 12 del Proyecto.

280 PEREZ GONZALEZ, M., en *La responsabilidad internacional (I): el hecho internacionalmente ilícito*, op. cit.; p. 860.

281 La CIJ consideró posible hacerlo bajo la óptica del D.I. consuetudinario, arguyendo al respecto que, «*aun cuando una norma convencional y una norma consuetudinaria que afecten al presente litigio tuvieran exactamente el mismo contenido, el Tribunal no vería en ello una razón para considerar que la intervención del proceso convencional deba necesariamente privar a la norma consuetudinaria de su aplicabilidad distinta*». Militarv and Puramilitary Activities in and against Nicaragua, doc. cit; par. 94. Así, tras sostener a propósito del uso de la fuerza por los Estados que tanto la Carta de las N.U. como el Derecho Internacional Consuetudinario «*proceden de un principio fundamental común que proscribe el uso de la fuerza en las relaciones internacionales*» (*ibid*.; par. 97) decidió, a la vista de los hechos considerados probados, que los Estados Unidos violaron respecto de Nicaragua, entre otras, las obligaciones de Derecho Internacional Consuetudinario de no intervenir en los asuntos

En el supuesto que nos ocupa, la anterior afirmación ha de entenderse crucial por dos motivos. El primero de ellos es que, como se viene manifestando, no existe todavía una norma convencional que reconozca, regule o limite el uso de internet como método de combate. En segundo lugar, porque, como consecuencia del hecho anterior, a falta de dicha norma expresa es necesario interpretar el Derecho vigente, de tal modo que vengan a colmarse las lagunas jurídicas existentes y, será la aplicación del DIH convencional y también consuetudinario, el modo en que ello deba hacerse.

Por lo tanto, siguiendo la lógica del enunciado del artículo 12 del Proyecto, la responsabilidad por un hecho ilícito de un Estado, puede originarse en un Tratado Internacional, sea éste bilateral o multilateral o bien, nacer de las exigencias impuestas por el Derecho Consuetudinario. Trasladada esta premisa, al ámbito que aquí se estudia, el origen convencional de la ilicitud de un hecho, derivado del uso de internet como método de combate habrá que buscarse en el DIH Convencional y Consuetudinario y, por lo tanto, en las obligaciones impuestas por los Convenios de Ginebra y en aquellas que viene recogidas en la Compilación de DIH consuetudinario.

Deben tenerse en cuenta, en este punto, las específicas normas que, sobre responsabilidad del Estado contiene el DIH, que han hecho pensar, incluso, en la autonomía del sistema de DIH, como se mencionaba en el primer Capítulo[282]. En concreto, el artículo 91 del PA I, establece que "*A Party to the conflict, which violates the provisions of the Conventions or of this Protocol shall, if the case demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part*

---

de otro Estado, de no recurrir a la fuerza contra otro Estado y de no atentar contra la soberanía de otro Estado (*ibid*.; par. 146-147).

282 El Manual de Tallin menciona, como ejemplo de ello, que el artículo 3 del IV Convenio de La Haya y el artículo 91 del PA I prevén una compensación en el caso de violación de ciertas normas de DIH y, así, afirma que "*A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation. 1. This Rule is based on the customary international law of State responsibility, which is largely reflected in the International Law Commission's Articles on State Responsibility. It must be noted, however, that the law of armed conflict contains a number of specific rules on State responsibility for violation thereof. In particular, Articles 3 of Hague Convention IV and 91 of Additional Protocol I provide for compensation in the case of a violation of certain rules of the law of armed conflict*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p. 36.

of its armed forces". Esta es una norma que puede asumirse como un principio general del Derecho Internacional.[283]

Por su parte, los Convenios de Ginebra prevén idénticas disposiciones. En concreto, cabe aquí traer a colación, el artículo 51 del I Convenio de Ginebra, el artículo 52 del II Convenio, el artículo 131 del III Convenio y el artículo 148 del IV Convenio. En todos los casos se prevé el específico régimen de responsabilidad internacional del Estado[284]. Del articulado de los citados Convenios, pues, se concluye que la violación de las normas de DIH, aplicables al combate, puede originar responsabilidad internacional, en aplicación del sistema autónomo de DIH recogido en los repetidos Convenios.

Así, de los supuestos citados en el mencionado artículo, puede decirse que el hecho de causar deliberadamente grandes sufrimientos o de atentar, gravemente, contra la integridad física o la salud, como la destrucción y la apropiación de bienes, no justificada por necesidades militares y que se efectúen a gran escala, ilícita y arbitrariamente, pueden ser ocasionados a través de un ataque cibernético. De este modo, puede surgir la responsabilidad internacional que tiene su origen en el Derecho Convencional.

La aplicación del DIH Consuetudinario a los medios y métodos de combate no ofrece duda, como puede concluirse del Capítulo Primero del presente trabajo. Tal como afirma el CICR, la "*amplia mayoría de las disposiciones que figuran en los Convenios de Ginebra, incluido el artículo 3 común, forma parte del derecho internacional consuetudinario*" y dado que "*actualmente 192 Estados son*

283 Los Comentarios al PA I, reflejan que "*Such a provision, which is indeed justified, corresponded to the general principles of law, on international responsibility. Moreover, any recourse by wronged persons to the law was considered illusory if this could not be exercised against the government of the perpetrators of these violations, through their own government*". SANDOZ, Y., SWINARSKI, Ch., ZIMMERMANN, B. (Ed.). Commentary on the Additional Protocols to the Geneva Conventions of 8 June 1977 to the Geneva Conventions of 12 August 1949. International Committee of the Red Cross. Geneva, 1987; p. 1090.

284 En concreto, estos artículos tienen el texto común que sigue: "*Ninguna Parte Contratante podrá exonerarse, ni exonerar a otra Parte Contratante, de las responsabilidades en que haya incurrido ella misma u otra Parte Contratante a causa de las infracciones previstas en el artículo anterior", es decir, las que implican uno cualquiera de los actos siguientes, si se cometen contra personas o bienes protegidos por el Convenio: el homicidio intencional, la tortura o los tratos inhumanos, incluidos los experimentos biológicos, el hecho de causar deliberadamente grandes sufrimientos o de atentar gravemente contra la integridad física o la salud, la destrucción y la apropiación de bienes, no justificada por necesidades militares y efectuadas a gran escala, ilícita y arbitrariamente*".

Partes en los Convenios de Ginebra, éstos son vinculantes para casi todos los Estados como derecho convencional[285]".

En el mismo sentido, de la Opinión Consultiva emitida por la CIJ a resultas del empleo de las armas nucleares, ha quedado claramente fijada la aplicación de una serie de normas de DIH al uso de las armas nucleares, por constituir DIH aplicable a todos los conflictos armados[286].

En aplicación de los criterios establecidos por la CIJ en su Opinión Consultiva, queda prohibido cualquier ataque contra personas civiles o bienes de carácter civil[287], los ataques indiscriminados, que serán aquéllos que no están dirigidos contra un objetivo militar concreto; en los que se emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o en los que se emplean métodos o medios de combate cuyos efectos no sea posible limitar conforme a lo exigido por el DIH y que, en consecuencia, en cualquiera de tales casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil[288]. Asimismo, queda prohibido lanzar un ataque, cuando sea de prever, que cause incidentalmente muertos y heridos entre la población civil, daños a bienes de carácter civil o ambas cosas, que sean excesivos en relación con la ventaja militar concreta y directa prevista. [289]Igualmente, es obligatorio que los métodos y medios de hacer la

285 HENCKAERTS, al respecto sostiene que, "*Por consiguiente, el objeto propiamente dicho del estudio no era la índole consuetudinaria de las disposiciones de los Convenios, sino más bien el examen de ciertas cuestiones reguladas por tratados que aún no han sido ratificados universalmente, en particular los Protocolos adicionales, la Convención de La Haya para la protección de los bienes culturales y algunas convenciones específicas que regulan el empleo de las armas*". Estudio sobre el derecho internacional humanitario consuetudinario: una contribución a la comprensión y al respeto del derecho de los conflictos armados. HENCKAERTS, J.-M., *Estudio sobre el derecho internacional humanitario consuetudinario: una contribución a la comprensión y al respeto del derecho de los conflictos armados.* International Review of the Red Cross, vol.87, núm. 857. Marzo 2005; pp. 1-50, en particular, p.16 y 17.

286 En opinión del CICR, las normas señaladas por la CIJ reflejan el Derecho Internacional Humanitario Consuetudinario y son aplicables en todos los conflictos armados. Las mismas han sido recogidas de forma sintetica en el documento, CICR, *Armas nucleares y Derecho Humanitario. Nota informativa 4*, doc. cit.

287 Normas 1 y 7, HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, vol. I, op. cit.; pp. 3-8 y 29-33. También, al respecto, véase el artículo 48 del PA I.

288 Normas 11 y 12, HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, vol. I, op. cit.; pp. 43-50 y el artículo 51 (4) del PA I.

289 Norma 14, *Ibidem*; pp. 53-57 y artículo 51 (5) (b) del PA I.

guerra se empleen, teniendo debidamente en cuenta, la necesidad de proteger y preservar el medio ambiente natural, tomando todas las precauciones factibles para no causar daños incidentales al medio ambiente o reducirlos, al menos, todo lo posible[290].

Por último, hay obligación de tomar las precauciones factibles en los ataques, de tal modo que las operaciones militares se realizarán con un cuidado constante de preservar a la población civil, a las personas civiles y los bienes de carácter civil. Se tomarán todas las precauciones factibles para evitar, o reducir en todo caso a un mínimo, el número de muertos y heridos entre la población civil, así como los daños a bienes de carácter civil, que pudieran causar incidentalmente. Las partes en conflicto deberán tomar todas las precauciones factibles en la elección de los medios y métodos de guerra para evitar, o reducir en todo caso a un mínimo, el número de muertos y de heridos entre la población civil, así como los daños a los bienes de carácter civil, que pudieran causar incidentalmente[291].

La responsabilidad internacional del Estado podrá surgir, pues, de una norma convencional de DIH que, además, ha sido llevada a la práctica y constituye DIH consuetudinario y puede ser exigida, tanto por la aplicación del sistema propio, como por el sistema previsto en el Proyecto de artículos.

Una vez acreditada la producción del hecho ilícito, por acción u omisión, en el modo que se estudió en el Capítulo precedente[292], surgen las obligaciones jurídicas que conforman la responsabilidad internacional del Estado que, a su vez, serán objeto de análisis en la segunda parte del presente del presente estudio. Sin embargo, en este punto, es preciso realizar una detenida mención al origen de esa responsabilidad, pues la violación de una norma internacional puede conllevar distintas consecuencias jurídicas, en función de la naturaleza de la misma.

Así, en virtud de lo dispuesto en el artículo 33 del Proyecto, las obligaciones propias de la responsabilidad internacional pueden existir con

290Norma 44, *Ibidem*; pp.163-168.
291Normas 15 y 17, *Ibidem*; pp. 59-63 y 65-67. También, el artículo 57 (1) y (2)(a)(ii), del PA I.
292 En este sentido, el artículo 28 del Proyecto establece: "*La responsabilidad internacional del Estado que, de conformidad con las disposiciones de la primera parte, nace de un hecho internacionalmente ilícito produce las consecuencias jurídicas que se enuncian en la presente parte*".

relación a otro Estado, a varios Estados o a la comunidad internacional en su conjunto, según sean, en particular, la naturaleza y el contenido de la obligación internacional violada y las circunstancias de la violación[293].

En consecuencia, deberá examinarse la naturaleza y contenido de las normas de DIH, al objeto de determinar si su violación, genera la correspondiente responsabilidad internacional, respecto de otro Estado, o por el contrario, nos encontramos ante la posibilidad de que dicha relación jurídica surja frente a varios Estados o, por último frente a la comunidad internacional en su conjunto.

En este sentido, hay que recordar que son indiscutibles los efectos *erga omnes*, de las normas comprensivas de DIH. Sin embargo, nos encontramos aquí ante la necesidad de ahondar en la naturaleza de dichas normas para determinar si, además, resultan normas de *ius cogens* y, por lo tanto, oponibles frente a la comunidad internacional en su conjunto. Es decir, la imperatividad de las normas de DIH frente a los Estados Parte de los Tratados que conforman el DIH convencional, resulta cuestionable, sin perjuicio de que la práctica reiterada, sin oposición por parte de los mismos, ha consolidado el DIH Consuetudinario.

Como consecuencia de lo anterior, la violación de una norma de DIH hará surgir la responsabilidad internacional frente al Estado o Estados infractores que se hallen entre los aquí citados. Sin embargo, de ello no puede colegirse que dichas normas puedan ser objeto de invocación, *per se*, por la Comunidad Internacional en su conjunto.

A la hora de esclarecer qué se entiende por obligaciones frente a la Comunidad Internacional en su conjunto, es necesario recoger el contenido del artículo 40, del mismo Proyecto, dedicado a las normas que resultan de aplicación, en relación a las violaciones graves de obligaciones emanadas de

293 La literalidad del artículo 33 del Proyecto es la que sigue: "*1. Las obligaciones del Estado responsable enunciadas en la presente parte pueden existir con relación a otro Estado, a varios Estados o a la comunidad internacional en su conjunto, según sean, en particular, la naturaleza y el contenido de la obligación internacional violada y las circunstancias de la violación.2. La presente parte se entiende sin perjuicio de cualquier derecho que la responsabilidad internacional del Estado pueda generar directamente en beneficio de una persona o de una entidad distinta de un Estado*".

normas imperativas del Derecho Internacional general[294]. Pues bien, esta distinción, realizada en función de la distinta naturaleza de la norma[295], comprende dos tipos de obligaciones: las obligaciones de un Estado frente a otro y las obligaciones de un Estado frente a la Comunidad Internacional en su conjunto, habida cuenta que "*de la importancia de los derechos en cuestión, puede derivarse un legítimo interés de todos los Estados en su protección*[296]".

Por lo tanto, en la constatación de un hecho ilícito como consecuencia de la violación de una obligación de DIH, a través de un ciberataque, habrá que plantearse si dicha obligación constituye una norma imperativa Derecho Internacional general, en orden a determinar si, la responsabilidad, por su violación, podrá ser ejercida, por toda la Comunidad Internacional en su conjunto o, únicamente, por el Estado o conjunto de Estados que sean parte del DIH Convencional o hayan observado una práctica sin oposición respecto del DIH consuetudinario.

El comentario al artículo 40 del Proyecto, en su párrafo 5, entiende que "*teniendo presente que la Corte Internacional ha definido como inconculcables las normas básicas de DIH aplicables en los conflictos armados, parecería estar justificado que se considerasen también imperativas*", reflejando, así, la existencia de los principios que se aquí se mencionan como de obligada observancia en el combate.

Sin embargo, la anturaleza imperativa de estas normas, es una cuetsion distinta que la CIJ abordo en su Opinion Consultiva y, sobre la quese volverá en el momento oportuno[297].

---

294 El artículo 40 del Proyecto establece: "*1. El presente capítulo se aplicará a la responsabilidad internacional generada por una violación grave por el Estado de una obligación que emane de una norma imperativa del derecho internacional general. 2. La violación de tal obligación es grave si implica el incumplimiento flagrante o sistemático de la obligación por el Estado responsable*".

295 La distinción a que se hace referencia es la formulada por la CJI en el caso Barcelona Traction Light and Power, doc. cit.; par. 30.

296 Así lo expresa el Comentario al Capítulo II del Proyecto.

297 En este sentido, la CIJ expresó, "*It has been maintained in these proceedings that these principles and rules of humanitarian law are part of jus cogens as defined in Article 53 of the Vienna Convention on the Law of Treaties of 23 May 1969. The question whether a norm is part of the jus cogens relates to the legal character of the norm. The request addressed to the Court by the General Assembly raises the question of the applicability of the principles and rules of humanitarian law in cases of recourse to nuclear weapons and the consequences of that applicability for the legality of recourse to these weapons. But it does not raise the question of the character of the humanitarian law which would apply to the use of nuclear weapons.*

Tambien el Preámbulo del Estatuto de Roma se pronuncia sobre "*los crímenes más graves de trascendencia para la comunidad internacional en su conjunto*" disponiendo, al respecto que " *no deben quedar sin castigo*" y, en consecuencia, que "*es deber de todo Estado ejercer su jurisdicción penal contra los responsables de crímenes internacionales*"; motivo por el que se establece "*una Corte Penal Internacional de carácter permanente, independiente y vinculada con el sistema de las Naciones Unidas que tenga competencia sobre los crímenes más graves de trascendencia para la comunidad internacional en su conjunto*[298]". Por lo tanto, en su momento habrá que plantearse si la violación de una norma de DIH, incluida en el ámbito de competencia del citado Estatuto[299], lo será o no, de una norma imperativa. En consecuencia, podría invocarse el artículo 40 del Proyecto, que declara de aplicación el capítulo III, relativo a las "*Violaciones graves de obligaciones contraídas en virtud de normas imperativas de Derecho Internacional General*".

De este modo, a contravención de las normas que, con más detalle serán analizadas posteriormente, conllevará la exigencia de responsabilidad internacional al Estado infractor y la misma y, en determinados casos, habrá que plantearse la posibilidad de que la misma sea ejercida por la Comunidad Internacional, en su conjunto, en el modo previsto en Proyecto[300].

5. VIGENCIA DE LA OBLIGACIÓN.

En el estudio de la responsabilidad internacional del Estado por hecho ilícito, como en cualquier otra relación jurídica, resulta determinante analizar la vigencia de la obligación, a que se halla sometido el Estado. Únicamente así, podrá establecerse si el mismo se hallaba, o no, compelido a su cumplimiento.

There is, therefore, no need for the Court to pronounce on this matter". Legality of the threator use of nuclear weapons, doc. cit.; par. 83.

298 Preámbulo del Estatuto de Roma de la Corte Penal Internacional, de 17 de julio de 1998, en vigor desde el 1 de julio de 2002. Doc. A/CONF.183/9.

299 El artículo 8 del Estatuto declara la competencia de la Corte para conocer de los crímenes de guerra, entendiendo por tales, las Infracciones graves de los Convenios de Ginebra de 12 de agosto de 1949, pasando el texto a enumerar los actos contra las personas o bienes protegidos por las disposiciones del Convenio de Ginebra pertinente. Estatuto de Roma de la Corte Penal Internacional.

300 El articulo 48.1 b) del Proyecto prevé que "*Todo Estado que no sea un Estado lesionado tendrá derecho a invocar la responsabilidad de otro Estado (…), si (…) la obligación violada existe con relación a la Comunidad Internacional en su conjunto. (…).*

Pues bien, en el presente caso se tratará de determinar la aplicación, en el tiempo de las normas de DIH que, como se ha visto obligan a todos los Estados, habida cuenta su carecer de normas erga omnes De este modo podrá comprobarse si, la violación de dicha norma por parte de un Estado, al empelar un ciberataque como método de combate, hace surgir la relación jurídica propia de la responsabilidad internacional.

El Proyecto de artículos establece que, el hecho ilícito de un Estado ha de tenerse, por violación de una obligación internacional, siempre y cuando dicho Estado se halle vinculado a la misma, en el momento de producirse el hecho. No obstante, la redacción, formulada en modo negacional, pudiera parecer más una causa de exclusión que una puntualización en relación a la vigencia de la norma[301]. En cualquier caso, resulta evidente la necesidad su vigencia.

En este sentido, PEREZ GONZALEZ, recuerda el laudo dictado el 4 de abril de 1928, en el asunto Isla de Palmas, que estableció que «*un hecho jurídico debe apreciarse a la luz del Derecho de la época y no del Derecho en vigor en el momento en que surge o ha de resolverse una controversia relativa a ese hecho*[302]».

En el caso de los ciberataques, la ausencia de normas convencionales, que regulen expresamente los ataques cibernéticos, en el sentido que aquí se recogen, podría originar el supuesto de que, con posterioridad al lanzamiento de una ciberoperación, se aprobara un Tratado que contemplara expresamente dicha actuación. En ese caso, podría, asimismo, surgir la duda de si el Estado se halla o no sujeto a la obligación internacional impuesta por dicho Tratado. En un caso como ese, sería preciso analizar la obligación internacional, en el modo en que aquí se ha venido exponiendo, es decir, teniendo en cuenta que, los métodos de

301 El citado artículo 13 del Proyecto de artículos, literalmente establece: "*Un hecho del Estado no constituye violación de una obligación internacional a menos que el Estado se halle vinculado por dicha obligación en el momento en que se produce el hecho*".

302 PEREZ GONZALEZ, asimismo, pone de manifiesto las conclusiones del Quinto Informe sobre responsabilidad internacional, del Relator Especial AGO. En dicho Informe, al respecto, puede leerse: "*If at the time of the conduct with which it is charged, the State is no longer under obligation, there can be no question of attributing to it "a breach of an international obligation" as provided for in draft article 3 (b) and of regarding it as having committed an internationally wrongful act*". Fifth report on State responsibility by Mr. Roberto Ago, Special Rapporteur, doc. cit. p.15, citado, asimismo, por PEREZ GONZALEZ, M., *La responsabilidad internacional (I): el hecho internacionalmente ilícito*.op. cit.; p.861

combate no pueden ser tratados, únicamente, a la luz del Derecho Convencional. No cabría duda, en este supuesto de la aplicabilidad del Derecho Consuetudinario, pero además, sería preciso, invocar el carácter de normas erga omnes e incluso, en determinados supuestos, de ius cogens, que el Comentario al Proyecto de artículos, otorga a las normas de DIH, de modo tal que dicha invocación podría ser realizada, en su caso, por la Comunidad internacional en su conjunto.

5.1 La posibilidad de que el ciberataque se manifieste como hecho ilícito continuado.

Especial interés, encuentran aquí, las normas relativas al comienzo del hecho ilícito y a la duración o prolongación de sus efectos pues, habrá que tener en cuenta las posibilidades de uso, que ofrece este método de combate. En los casos que hasta ahora se han citado, resulta evidente que el lanzamiento del ciberataque, que podríamos considerar un hecho ilícito, si reuniera los caracteres vistos en el Capítulo Primero, dista en el tiempo respecto de la producción de sus efectos. En casos como el ocurrido en Estonia, los ciberataques se produjeron de forma continua, pero requirieron la repetición de los ataques, por parte de los atacantes. Así, si éstos no actuaban, el hecho no se producía y tampoco sus efectos. Idéntico es el supuesto, en el sentido que aquí se expresa, en relación a los ataques que sufrió la página web de la emisora Radio Free Europe/Radio Liberty en Bielorusia [303]. Sin embargo, en el caso del virus Stuxnet esta circunstancia no se aprecia de una forma tan clara, pues los efectos del ciberataque se estuvieron produciendo, de forma continua, desde la introducción del virus en la central nuclear de Irán hasta, al menos, el momento en que el mismo fue detectado.

Pues bien, el artículo 14 del Proyecto establece que "*La violación de una obligación internacional mediante un hecho del Estado que no tenga carácter continuo tiene lugar en el momento en que se produce el hecho, aunque sus efectos perduren*". En

303 En el sentido expuesto, anteriormente se expresan, TIKK, E. TASKA, VHUL, International cyberincidents. Legal Considerations, op. cit.; pp. 39-40.

los supuestos que aquí se contemplan, la posibilidad de denunciar un hecho ilícito, al ser violada una obligación de DIH, se circunscribe al momento en que se produce el ciberataque. En una interpretación literal del artículo transcrito, una vez terminado el ataque, pese a que los efectos del mismo persistan, no podrá entenderse que se sigue produciendo el hecho ilícito y, únicamente, podrá ser exigida responsabilidad al Estado si, en el momento del ataque, se hallaba vinculado por la obligación internacional.

Esta disposición resulta especialmente relevante, en el contexto que aquí se examina, relativo al armamento virtual, pues éste permite la planificación, tanto del ataque, como de la duración de sus efectos. Además, el ataque cibernético permite ser ocultado, de tal modo que sus efectos se produzcan pasado el momento inicial del ataque. Y, aún más, puede ocurrir que, aun produciendo el daño perseguido con carácter inmediato, éste no sea descubierto por el Estado receptor del mismo hasta pasado un tiempo como ocurrió, también, con el lanzamiento del virus Flame[304]. En casos de estas características, como la introducción de virus de la naturaleza de Flame o Stuxnet, podrá surgir la duda de si, nos encontramos ante hechos puntuales, que producen efectos prolongados, o bien, ciberataques continuos, en el sentido expuesto en el párrafo segundo del mismo artículo.

Tampoco puede obviarse el hecho de que, el uso de internet, como método de combate, también podrá dar lugar a situaciones, como la descrita en el párrafo segundo del artículo 14 del Proyecto que, al tratar del hecho continuo establece que "*La violación de una obligación internacional, mediante un hecho del Estado que tiene carácter continuo, se extiende durante todo el período en el cual el hecho continúa y*

304 Sobre este tema, se ha pronunciado CARO BEJARANO, afirmando: "*Flame es un gusano de ciberespionaje altamente sofisticado que ha afectado a ordenadores de muchos países de Oriente Próximo y Europa del Este*"; "*No destruye como hacía el virus Stuxnet sino que espía de manera invisible, por ello, es más peligroso y difícil de detectar*". CARO BEJARANO, M.J. *Flame: una nueva amenaza de ciberespionaje*. Documento Informativo 34/2012 . Instituto Español de Estudios Estratégicos. Documento de fecha 13 junio de 2012; p.2. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI34-2012_Flame_Ciberespionaje_MJCB.pdf. Fecha de consulta, enero de 2013. También sobre dicho virus, se han pronunciado otros autores en el sentido siguiente: "*Also, Flame was quite unusual as a malware in the sense that it was an order of magnitude larger than typical malware samples (both for generic and targeted attacks*" BENCSATH B., et al., *The Cousins of Stuxnet*: *Duqu, Flame, and Gauss*, op.cit.

se mantiene su falta de conformidad con la obligación internacional". Es decir, en el supuesto de que una operación fuera lanzada, utilizando armas cibernéticas, desde el momento de su lanzamiento hasta la finalización del mismo se estaría violando la norma de DIH correspondiente, por ejemplo, la relativa a la imposibilidad de causar males innecesarios. Y ello se produciría, con independencia de cuál fuera el momento en que el Estado en cuestión se apercibiera de tal hecho.

En los casos antes citados habrá que analizar, además, si, el hecho de introducir un virus que, de forma constante, está afectando a la operatividad de determinadas redes o sistemas de otro Estado, se considera un hecho puntual de efectos prolongados o bien, un hecho continuo. En este sentido, el Comentario al Proyecto ofrece una serie de ejemplos, en relación a los hechos continuos, que parecen indicar que nos encontramos ante la segunda valoración. El comentario entiende que hechos ilícitos continuados son, por ejemplo, detener ilegalmente a un funcionario, ocupar ilegalmente parte del territorio de otro estado o desplegar Fuerzas Armadas en otro Estado sin su consentimiento, entre otros [305]. Evidentemente, mientras dichas situaciones fácticas se estén produciendo, también el hecho ilícito se está produciendo. Si bien es cierto que los ejemplos que ofrece el Comentario se limitan a situaciones, en que el hecho ilícito es físicamente comprobable, ello no impide que se considere que, la introducción de un virus informático como los que han sido citados, sea un hecho continuado. De esta forma, en cualquier momento en que se detectara la actuación de dicho virus podría invocarse, si así ocurriera, la violación de la obligación de DIH correspondiente.

De acuerdo con el Proyecto y, en los términos expuestos en el capítulo Primero, la producción del hecho ilícito podrá darse, no solo a través de una conducta activa, sino, también, omisiva. Por lo tanto, en este punto habrá que volver sobre dicha argumentación para constatar en qué momento se entiende cometido el hecho ilícito, por omisión y analizar, en consecuencia, la vigencia de la obligación internacional, a la que se halla sujeto el Estado. Conforme quedó

305 Comentario al artículo 14 del Proyecto.

expuesto, el Estado puede ser responsable internacionalmente, por omisión, en las situaciones en que no evite el hecho ilícito, pudiendo y debiendo hacerlo y, con ello, se produzca la violación de una norma de DIH, bien por el propio Estado, a través de un sujeto que actúe en nombre del Estado, bien por terceros, que consigan lanzar un ciberataque contra dicho Estado.

Pues bien, en ese sentido, la responsabilidad por omisión, contemplada y admitida por el Proyecto, se encuentra, asimismo, condicionada a la vigencia de la obligación internacional en cuestión. Así, la conducta omisiva del Estado se realizará desde el momento en que se produzca "*el acontecimiento y se extiende durante todo el período en el cual ese acontecimiento continúa y se mantiene su falta de conformidad con esa obligación*"[306]. La responsabilidad del Estado, pues, se produce durante todo el tiempo en que, el mismo, se encuentra en una situación pasiva permitiendo, de ese modo, la violación de una obligación internacional.

En este caso, será determinante analizar la conducta observada por el Mando militar pues, al hablar del hecho ilícito cometido por omisión, será preciso examinar si, en el momento de entrar en combate, el uso de las ciberarmas era, o no, debidamente controlado por el mismo. En el caso de que no se realizara ningún control sobre el empleo de dicho armamento, podría darse la responsabilidad por dicha omisión, desde el lanzamiento de una ciberoperación, que violara una norma de DIH, hasta que dejara de producirse esa violación. Para ello, asimismo, habrá que tener presentes las consideraciones antes realizadas en relación a los hechos ilícitos continuados. De esta manera, seguiría dándose la responsabilidad por omisión si, conociendo la introducción de un virus informático que, por ejemplo, produjera daños desproporcionados en relación con la ventaja militar, o que de otra manera infringiera una norma de DIH, en el modo que se verá en el epígrafe posterior. En relación a esta concreta responsabilidad exigida al Mando, procede traer de nuevo a colación la sentencia del Tribunal Penal para la Ex Yugoslavia que, en el caso *Tadic*, como pone de

306 Artículo 14 del Proyecto.

manifiesto SALMÓN, [307] señaló que: «*El alcance temporal y geográfico de un conflicto armado se extiende más allá del momento y lugar exacto de las hostilidades*». Asimismo, es importante destacar que, en atención a la esencial naturaleza protectora de las normas de DIH, se prevé la extensión de su aplicación, una vez finalizado el conflicto, siempre que existan "*víctimas detenidas por motivos relacionados con el conflicto*[308]", tal como prevé el PA II.

Asimismo, podría exigirse responsabilidad al Estado, que no impide el ataque a sus nacionales o bienes. Conforme a las obligaciones exigibles al Estado, en relación a la provisión de seguridad que ya han sido expuestas, la anterior argumentación sería, asimismo, de aplicación durante todo el tiempo en que durara el ilícito. Podría darse el supuesto de un incumplimiento, por parte del Estado, de las obligaciones a que viene sujeto por la normativa, que ha sido citada en el Capítulo precedente, en relación a la protección de infraestructuras críticas y que será objeto de examen, nuevamente, al tratar la atribución del hecho ilicito. Igualmente, podría darse el supuesto de inacción de un Mando militar que, durante el combate, incumpliera con las obligaciones impuestas expresamente al Mando Conjunto de Ciberdefensa[309].

---

307 Para la citada autora "*(…) teniendo en cuenta que el conflicto armado implica necesariamente violencia armada, la aplicación del DIH comienza con la apertura de hostilidades (y no con la amenaza de hacerlo) y termina después del cese de hostilidades cuando concluyan las operaciones militares, es decir, la ocupación misma, de existir*". SALMÓN, E. Introducción al Derecho Internacional Humanitario, op. cit.; pp. 85 y 86.

308 SALMÓN, Introducción al Derecho Internacional Humanitario, op. cit.; pp. 85 y 86.

309 La Orden Ministerial 10/2013, por la que se crea el MCCD determina, en su artículo 5, que sus cometidos son los siguientes: "*1. Garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios. 2. Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.3. Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques. 4. Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad. 5. Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. 6. Dirigir y coordinar, en materia de ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y el de operaciones de seguridad de la información del Ministerio de Defensa. 7. Ejercer la representación del Ministerio de Defensa en materia de Ciberdefensa militar en el ámbito nacional e internacional. 8. Cooperar, en materia de ciberdefensa, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de ciberseguridad en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional. 9. Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa*".

El caso de los ciberataques producidos en Bielorusia, a los que antes se ha hecho alusión, la responsabilidad por omisión resulta evidente, por más que dicho Estado no se hallara en un conflicto armado, ni se violara una norma de DIH a través de los ataques dirigidos a la emisora de radio aludida. Sin embargo, si puede afirmarse que se infringió una norma relativa al Derecho de los Derechos Humanos, como es la libertad de expresión, que no se vio amparada ni protegida por el Estado. En el supuesto de que, una situación de idéntica inacción, se hubiera producido, durante un conflicto armado internacional o no internacional, nada impediría la denuncia de ese hecho ilícito cometido por omisión[310].

5.2 El ciberataque como hecho ilícito compuesto.

El artículo 15 del Proyecto prevé, de forma expresa, la posibilidad de que, la acción u omisión ilícita, que origina la relación jurídica, propia de la responsabilidad internacional del Estado, esté constituida por una "*serie de acciones u omisiones, definida en su conjunto como ilícita*" y tiene lugar "*cuando se produce la acción u omisión que, tomada con las demás acciones u omisiones, es suficiente para constituir el hecho ilícito*". Según el párrafo segundo del mismo artículo, se entiende que la violación se está cometiendo "*durante todo el período que comienza con la primera de las acciones u omisiones de la serie y se prolonga mientras esas acciones u omisiones se repiten y se mantiene su falta de conformidad con la obligación internacional*".

En el caso que aquí se estudia, resulta necesario volver a retomar las consideraciones que, sobre el conflicto híbrido, fueron realizadas en el Capítulo precedente. En los conflictos que se libran en la actualidad y, en aquéllos, en los que resulta previsible la utilización de los ciberataques, como método de combate, parece probable que nos encontremos con una conjunción de factores, que originen un hecho ilícito internacional. Es decir, ya se ha apuntado en qué medida el ciberterrorismo podría entrar dentro de la aplicación del DIH, pues no

310 TIKK, E. TASKA, K., VHUL, L., International cyberincidents. Legal Considerations, op. cit.; pp.43-46.

puede olvidarse que este tipo de actividad podrá jugar un papel esencial, incluso, en conflictos que respondan a una concepción clásica de los mismos. Habrá que tener presente, así, que, aun cuando dichos conflictos se libren entre combatientes, respetando la protección, que el DIH otorga a los no combatientes, habrá supuestos de insurgencia o terrorismo, que obliguen a considerar la pérdida de protección de dicho estatuto. Pues bien, será probablemente en estos supuestos donde el factor cibernético pueda jugar un papel esencial en la configuración de un hecho ilícito compuesto.

A tenor de lo dispuesto en el Comentario de artículos, nos encontramos ante la violación de obligaciones que abarcan "*un conjunto de comportamientos y no a hechos concretos en sí*[311]". Por ello, no parece improbable que uno de esos comportamientos esté constituido por un ciberataque. No obstante, el propio Comentario limita la aplicación de esta figura, a los casos más graves de violaciones de obligaciones internacionales y ofrece ejemplos de supuestos, en los que el hecho ilícito necesita de varias acciones, para que llegue a consumarse, citando así, el Comentario al articulo 15, "*las prohibiciones del genocidio, el apartheid o los crímenes de lesa humanidad, los actos sistemáticos de discriminación racial, los actos sistemáticos de discriminación prohibida por un acuerdo comercial, etc*".

La enumeración, aquí citada, no puede llevar a confusión, a pesar de que los ejemplos que se ofrecen respondan a la evitación de conductas que, esencialmente, requieren una actividad física. De forma evidente, no será posible cometer un genocidio a través de medios virtuales. Sin embargo, en todas las conductas citadas, dicho elemento, puede contribuir de forma significativa. El apartheid, por ejemplo, podría verse favorecido a través de redes informáticas si, como pasó en los Estados que aquí han sido mencionados, las páginas web oficiales de un Estado fueran manipuladas, de forma que se transmitiera un mensaje, en ese sentido. Lo mismo cabe decir de los actos de discriminación racial, o de discriminación prohibida por un acto comercial. Precisamente, el citado Comentario, al respecto, entiende que son supuestos en los que el Estado ha

311 Comentario al artículo 15 del Proyecto.

"*adoptado una política o práctica sistemática*[312]". Pues bien, nada impediría que ellos se llevaran a cabo a través de la red y, aun menos, utilizando los métodos que son propios del ciberterrorismo. Con toda probabilidad, la actuación en la red caería dentro del ilícito internacional, por sí misma, si, en efecto, se produjera un caso de ciberterrorismo. Al respecto, ya se ha indicado que, en determinados supuestos, se prevé la aplicación del DIH pero, además, podría ser considerada un factor constitutivo de ese hecho compuesto, si se demostrara la intencionalidad, específica, de contribuir a alguna de las conductas, que se señalan, de modo expreso, en el párrafo anteriormente transcrito.

Sin embargo, esa específica intencionalidad se revelará, siempre, con carácter posterior, pues no será hasta el momento de valorar el hecho ilícito en conjunto, cuando se pueda comprobar la conexión, entre todos los ilícitos que lo componen. Por ello resultará determinante la persecución de dichas conductas, en función del ámbito jurídico que, a cada una, sea de aplicación, con independencia de que, posteriormente, se pruebe la comisión del hecho ilícito compuesto. Éste se producirá, a tenor de lo dispuesto en el artículo 15, en "*el momento en que se produce la última acción u omisión que, tomada con las demás acciones u omisiones, es suficiente para constituir el hecho ilícito sin que sea necesario que se trate de la última acción u omisión de la serie*".

Por otra parte, resulta determinante lo dispuesto en el párrafo segundo del artículo que se examina, que considera que el momento en que se produce la violación de la obligación internacional "*es el momento en que se produjo el primer hecho de la serie*".

Es decir, con independencia de que, hasta la finalización del hecho compuesto, no se tendrá prueba ni constancia del mismo, ello no obsta a que, una vez probado, se tenga por producido, desde el momento en que se produjo el primer ilícito. En el caso que nos ocupa, esta precisión resulta realmente relevante pues, en determinadas ocasiones, el lanzamiento de un ciberataque podrá constituir un primer hecho ilícito. Las ventajas de ejecución, que aquí se han ido exponiendo, llevan a considerar que, en efecto, puede ser la primera de las

312 Comentario al artículo 15 del Proyecto.

acciones a desarrollar en el tiempo. Sin embargo, cuando el hecho ilícito se tenga por completado, la acción inicial será la que determine el momento de ejecución del mismo. En este sentido, puede traerse de nuevo a colación el caso de los ataques sufridos por los usuarios de la estación de radio bielorrusa que han sido citados. Un ataque como este, claramente tendente a manifestar una postura política o ideológica, podría, en otro contexto, formar parte de un hecho ilícito compuesto si, posteriormente, dicha finalidad se manifestara, además, en otro tipo de actividades, que conllevaran la comisión de actos constitutivos, por ejemplo, de apartheid.

No puede tampoco olvidarse que, el hecho ilícito compuesto podrá darse en el desarrollo del combate. Como inmediatamente se verá, el contenido de la obligación internacional en este ámbito, está configurado por las limitaciones que, el DIH impone al uso de los métodos de combate. Pues bien, si a través de un ciberataque se violara dicha obligación internacional, atacando, por ejemplo, redes informáticas civiles incumpliendo, así la obligación de respetar al no combatiente, nada impediría que, posteriormente, dicha actuación fuera valorada como integrante de un hecho ilícito compuesto, si respondiera a la misma finalidad, que otras que se ejecutaran, a través de métodos de combate convencionales. De este modo, la ilicitud del hecho se estaría produciendo desde esa primera acción, hasta la comprobación de la última de ellas, que resultara necesaria, para acreditar el hecho ilícito compuesto, con independencia de que, como prevé el artículo transcrito, "*se trate* (o no) *de la última acción u omisión de la serie*". Por último, también habrá que considerar que, como ya se ha puesto reiteradamente de manifiesto, los efectos de un ciberataque podrían seguir produciéndose, una vez terminado el lanzamiento del mismo.

6. CONTENIDO DE LA OBLIGACIÓN INTERNACIONAL INFRINGIDA.

Una vez delimitado el carácter internacional de la obligación jurídica, es necesario abordar el papel que juega el DIH, al aportar el contenido del elemento objetivo de la misma, en el plano de la responsabilidad internacional. Es decir, una vez delimitado el carácter internacional de la obligación infringida, así como

su vigencia en el tiempo, corresponde, en este momento, entrar a estudiar el contenido concreto de dicha obligación para, así, entrar a determinar, en qué supuestos se dará la violación de la obligación, al utilizar los ciberataques, como método de combate.

En este sentido, será preciso, nuevamente, realizar una interpretación de las normas que, desde antiguo, vienen aplicándose a los conflictos amados internacionales y no internacionales, para determinar en qué modo y supuestos, las mismas son aplicables a los ataques cibernéticos.

En el presente estudio, ceñido a la aplicabilidad del DIH como originador de responsabilidad internacional, es preciso comenzar haciendo especial mención al contenido del artículo 1, común a los cuatro Convenios de Ginebra y al PA I, conforme a los que, todos los Estados se comprometen a "*hacer respetar*" sus disposiciones "*en todas las circunstancias*". En la actualidad, dicha afirmación es interpretada, de forma unánime, en el sentido de que, el referido artículo se refiere a violaciones, cometidas por los Estados. Si bien ya se ha mencionado que, en el asunto *Nicaragua* la CIJ sostuvo que dicho artículo da expresión específica a un "*principio general del derecho humanitario*" dicha afirmación "*no resulta de los Convenios en sí, sino también de los principios generales del Derecho internacional humanitario de los que los Convenios no son más que la expresión concreta*[313]". Este principio se aplica, también, al derecho de los conflictos armados no internacionales, aunque no parece dejar claro qué Estados pueden tomar medidas al respecto, ni tampoco, qué medidas y, según qué procedimiento, pues como afirma SASSOLI, "*el artículo 1 común aplica, en algunos aspectos, las normas generales sobre la responsabilidad de los Estados y, en otros, establece una norma secundaria especial; además, es una norma primaria a la que se aplican las normas sobre la responsabilidad estatal*". De este modo, habrá que establecer, en qué momento, un Estado puede considerarse lesionado, por una infracción del DIH para, en

313 En este sentido se pronuncia COMELLAS AGUIRREZÁBAL, M.T., *La contribución del Consejo de Seguridad de las Naciones Unidas a la aplicación y al desarrollo normativo del Derecho Internacional Humanitario.* Revista Española de Derecho Militar Número 85; pp. 175-212, en particular, p.181.

razonamiento del mismo autor, "*explicar cómo puede reaccionar un Estado lesionado y qué medidas, si las hay, pueden aplicar otros Estados*"[314].

En este punto, asimismo, resulta relevante la mención al Consejo de Seguridad de Naciones Unidas, pues, como afirma COMELLAS, dicha Organización "*ha tenido un especial protagonismo e interés en el desarrollo del contenido del DIH, así como en el esfuerzo por enfatizar su aplicación*[315]". De este modo puede compartirse la afirmación de que la Organización de Naciones Unidas "*ha llevado a cabo una importante contribución: por una parte, al adoptar resoluciones y decisiones, el Consejo de Seguridad ha participado en la consagración y reafirmación de normas de Derecho humanitario; por otra, la creación y el recurso a ciertos mecanismos y procedimientos dirigidos a hacer respetar el Derecho humanitario pueden contribuir a la efectiva aplicación de sus normas.*"[316]

6.1. Los límites impuestos por el DIH a la conducción de las hostilidades, aplicables a los ciberataques.

De la ausencia de un régimen jurídico que regule expresamente el uso de los ataques informáticos, en la conducción de operaciones, en ningún caso, se puede colegir la posibilidad de un uso ilimitado de los mismos. Es necesario, por lo tanto, reflexionar sobre cuáles hayan de ser esos límites, que se imponen y, analizar la justificación de los mismos. En esta labor, el precedente sentado por la regulación de las armas nucleares y las conclusiones alcanzadas, por la CIJ, suponen la principal referncia. Tampoco puede olvidarse, en este aspecto, las declaraciones formuladas al respecto por el CICR. Por ello, es preciso examinar aquéllas normas de DIH consuetudinario, cuya aplicación resulta obligatoria, en todo conflicto armado y, de este modo, sentar las bases, que permitan perfilar los requisitos de licitud, de la actuación de un Estado, al intervenir en un

314 Así puede leerse en SASSÒLI, M. *La responsabilidad del Estado por las violaciones del derecho internacional humanitario*, op. cit.

315 Así lo entiende COMELLAS AGUIRREZÁBAL, quien, igualmente, afirma que "*La acción del Consejo de Seguridad ha servido para introducir nuevas dimensiones a la obligación de hacer respetar el DIH*". COMELLAS AGUIRREZÁBAL, M.T., *La contribución del Consejo de Seguridad de las Naciones Unidas a la aplicación y al desarrollo normativo del Derecho Internacional Humanitario*, op.cit.; pp. 178 y 191

316 *Ibidem*; pp. 178 y 191.

determinado conflicto para, en Capítulos posteriors, abordar el estudio de las consecuencias derivadas de su transgresión.

La aplicación del DIH, en el ámbito informático, se justifica en la posibilidad real de los ataques cibernéticos y sus potenciales efectos devastadores, en la población e infraestructuras críticas, tales como sistemas de control aéreo o de suministro de agua o electricidad[317]. La licitud de los nuevos medios y métodos bélicos, en general, dependerá de su empleo, pero no queda excluida la posibilidad de que, algunas armas, que se consideren inherentemente indiscriminadas o, que causen sufrimientos superfluos o innecesarios, deban ser prohibidas[318]. La consideración de los ataques informáticos como un arma de guerra es una cuestión que no ofrece duda para el CICR, que, en este sentido, afirma que: "(…) *no cabe duda de que el Derecho Internacional Humanitario abarca la guerra informática* (…)"[319], por cuanto el uso de la fuerza no tiene por qué venir referido, exclusivamente, a la fuerza cinética, sino que podrá ampliarse a cualquier modo de causar un daño en personas o bienes[320].

Una vez sentada la anterior premisa, resultante de la consideración de internet como un medio de combate, resta dirimir los métodos de combate, que resultarán lícitos, de conformidad con el DIH. Es decir, siguiendo la tradicional distinción, entre medios y métodos de combate[321], cabe concluir que internet pertenece a la primera categoría y el modo en que éste se emplee, entrará dentro de la segunda. Será preciso analizar la doctrina contemporánea, relativa a la licitud de estos métodos, a la hora de determinar si un Estado, en el empleo de

317 Así quedó puesto de manifiesto en CICR, *International Humanitarian Law and New Weapon Technologies*. Statement 34th Round Table on Current Issues of International Humanitarian Law, doc. cit.

318 SPOERRI, P. en "*Mesa redonda sobre el DIH y las nuevas tecnologías armamentísticas – Conclusiones*", de 13 de septiembre de 2011. Documento disponible en el sitio web: https://www.icrc.org/spa/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm. Fecha consulta mayo 2013.

319 Asi lo contempla el CICR en el documento, *Guerra informática*, de 20 de octubre de 2010. Documento disponible en el sitio web: www.icrc.org/spa/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare. Fecha consulta: noviembre 2013.

320 Así se expresa, también, HUGHES, R. *A treaty for cyberspace,* op. cit; pp. 523-541.

321 Esta distinción viene recogida por CASANOVAS Y LA ROSA, O. *El Derecho Internacional Humanitario en los conflictos armados (I): Objetivos militares, métodos y medios de combate*. DIEZ DE VELASCO, M. Instituciones de Derecho Internacional Público. Tomo I, Tecnos. Madrid 2013; pp. 1097-1121, en particular, p. 780.

los mismos, ha incurrido en responsabilidad por su inobservancia, en su defecto, alguien que lo ha hecho como "agente" de ese Estado, y no con carácter particular.

No obstante, como se verá posteriormente, la responsabilidad indirecta se podrá exigir siempre que el particular haya actuado como tal, sin ser comisionado por el Estado, pero con su consentimiento, o al menos, sin que se haya tomado medida alguna para prevenir tal actuación. Aun así, para ejercer el derecho al uso de la fuerza por parte del Estado agredido, habrá que considerar, previamente, el nivel de implicación del Estado del que surja la agresión del particular, toda vez que la mera tolerancia o inactividad no podría dar lugar a un uso de la fuerza contra el mismo. Hasta la fecha, ésta ha sido una cuestión crucial, ya que, tanto en los ataques sufridos por Estonia como por Georgia, resultó imposible determinar que los particulares identificados como atacantes lo hicieran por cuenta de un Estado, pese a que la Federación Rusa mostró su apoyo a los mismos de un modo evidente.[322]

En este sentido, resulta de suma importancia tener en cuenta la aplicabilidad del DIH Consuetudinario, como conjunto de normas, derivadas de una práctica general aceptada como norma de Derecho. Puesto que no resulta necesario que los Estados acepten de un modo formal una norma consuetudinaria, para que la misma adquiera un carácter vinculante para ellos, se impone la exigibilidad universal de las normas que componen este Derecho Consuetudinario, salvo los supuestos de objeción persistente.

La utilización de internet, como un medio de combate exigirá, pues, que el mismo, responda a una necesidad militar, que en su empleo se observe la necesaria distinción entre combatientes y no combatientes; su uso resulte proporcional al objetivo perseguido, no se incurra en perfidia y, por último,

322 Respecto al origen de todos estos ataques, a juicio de las empresas privadas que se ofrecieron a estudiarlos, tales como Arbor Networks´o el proyecto Grey Goose, pronto se llegó a la conclusión de que el origen de los ataques se encontraba en Rusia y de que se había producido de una forma totalmente organizada, utilizando hasta seis servidores distintos para lanzarlos. Así se pone de manifiesto por parte de TIKK, E., KASKA, K. VIHUL, L., International Cyberincidents, op. cit.; p. 23.

respete la neutralidad de terceros. Es decir, que serán de aplicación las normas convencionales y consuetudinarias relativas a la conducción de hostilidades.

6.1.1 La necesidad militar del ataque.

La licitud del ataque informático dependerá, en primer lugar, de que éste responda a una necesidad militar, es decir, que se produzca como consecuencia de la necesidad de conseguir un objetivo militar, de forma que, el ataque contribuya, directamente, al combate.

Este concepto ha sido tratado desde antiguo y, ya en el Código de Lieber de 1863, era definido como «*the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war*»[323]. Este incipiente cuerpo de Derecho Humanitario, advertía de la obligación de evitar las conductas, demostrativas de crueldad, en la persecución del objetivo militar, de forma que, este primer requisito, en ningún caso, puede entenderse como una autorización absoluta o carente de límite. Antes bien, como recuerda GEISS, será preciso que esa necesidad militar se equilibre con el principio de humanidad[324].

En virtud del principio de proporcionalidad, serán ilícitos los ataques que, aun dirigidos a un objetivo militar, puedan suponer la pérdida de vidas humanas, daños a civiles, daños a objetos civiles o una combinación de los anteriores, cuando resulten excesivos, en relación con la ventaja militar concreta y directa, que se prevé alcanzar. De este modo, el principio queda configurado como una limitación, cuya aplicación, inevitablemente, dependerá del juicio subjetivo que se realice, en cuanto a la valoración de esos posibles daños[325]. Obviamente, no cabrá duda sobre la ilicitud del ataque cuando el mismo carezca por completo de

323 El Código que se cita, comunmente conocido como codigo Lieber, se trata del documento, *Instructions for the Government of Armies of the United States in the Field* (Lieber Code). 24 April 1863.
324 Así se afirma por parte de GEISS, R. en *Las estructuras de los conflictos asimétricos*, op. cit; p. 12.
325 SASSÒLI M., BOUVIER A. A., QUINTIN A. How does law protect in war?. Cases, Documents and Teaching Materials on Contemporary practice in International Humanitarian Law. Part I, Volume I Outline of International Humanitarian Law. ICRC; Capítulo 9; p. 9.

esa necesidad, por no reportar ninguna ventaja militar, a la parte en el conflicto que realiza tal ataque[326].

En los ejemplos que se han sido exponiendo, a lo largo del presente estudio, puede apreciarse que dicha necesidad militar estaba presente, en alguno de los más relevantes. Es evidente que existía en los ciberataques, recibidos por las Fuerzas Armadas de Georgia, en el año 2008, habida cuenta que dicho Estado, se hallaba en combate y que, la interferencia en las comunicaciones de las Fuerzas Armadas contribuye a la derrota militar y sumisión del enemigo; entendidos ambos elementos como definitorios de la necesidad militar del ataque[327]. Sin embargo, en el caso del lanzamiento del virus Stuxnet, la necesidad militar puede no resultar tan evidente, en primer lugar porque Irán no se hallaba librando ningún combate y, en segundo lugar, porque, al resultar desconocida la autoría del ataque, se ignora la finalidad última de los atacantes. No obstante, el objetivo perseguido y, finalmente, logrado, consistente en la paralización de la actividad nuclear de Irán, podría corresponder a dicha necesidad militar, en el caso de haberse producido en un contexto bélico.

Distinta sería, sin embargo, la respuesta en los casos de los ataques recibidos tanto por Estonia como por Letonia. En estos supuestos, no nos encontramos ante el desarrollo de ciberoperaciones, en el transcurso de un conflicto, ni ante un caso de ciberguerra. Sin embargo, si de los mismos se hubiera derivado un posterior conflicto, nos encontraríamos ante un claro ejemplo de conflicto asimétrico, originado por un ciberataque, potenciador del conflicto, en los términos, anteriormente expuestos. La asimetría de los actuales conflictos, ha propiciado una nueva valoración del principio de necesidad militar, dado lo imprescindible del mismo, a la hora de observar la necesaria proporcionalidad del ataque, impuesta por los artículos 51 y 57 del PA I[328]. De

326 Esta es la conclusión que puede extraerse, entre otras de la Sentencia dictada en el caso Rajic, cuya condena se justifica, entre otros motivos, en esa falta de necesidad militar del ataque perpetrado a la población de Stupni Do. En palabras del Tribunal "*…Stupni Do had no military signifiance.*"; "*…There is no evidencethat there was a military instalation or any other legitímate target in the village…*". The Prosecutor v. Rajic, Case n. IT-95-12-R61, YCTY, September 1996.

327 GEISS, R. *Las estructuras asimétricas*, op. cit.; p. 13.

328 Artículo 57 del PA I. Por su parte, el artículo 51 establece esa obligación de observar la proporcionalidad, especialmente, en sus apartados 4 y 5 en los que prohíbe los ataques

hecho, si hay un conflicto que pueda resultar, a todas luces asimétrico, será aquél en que intervenga el elemento cibernético, bien por la disparidad de los medios técnicos a disposición de distintos Estados, bien porque, en un conflicto armado de carácter no internacional, una de las Partes, libre el mismo, a través de internet, procurando así una evidente asimetría entre ambas Partes. Pues bien, en este contexto, esa necesidad militar resulta de obligada observancia al resultar, en esencia, una limitación al uso de la fuerza.

De igual modo, podría aplicarse esta misma conclusión si, como consecuencia de los ciberataques, sufridos por la página web de la emisora Radio Free/Radio Liberty, radicada en Bielorusia, hubiese estallado un conflicto armado no internacional. La asimetría del mismo hubiera sido evidente, por cuanto los ataques provinieron del propio Estado, en el que la emisora se halla radicada y se lanzaron contra la página web de una entidad civil. En este supuesto, la necesidad militar no parece tan evidente, aunque tal y como afirma GEISS, "*a medida que aumenta la asimetría entre los beligerantes, la distinción entre las necesidades y los objetivos políticos y militares se difumina cada vez más*"[329].

Este último es un claro caso en el que, el objetivo político resultó evidente, por cuanto se pretendió silenciar una reivindicación social, atinente a una actuación, de la que se hacía responsable al Gobierno de ese Estado y que, dicho Gobierno, procedió a silenciar, a través de la inutilización del canal, del que los manifestantes disponían, para hacerla valer. En este caso concreto, el umbral de violencia no fue sobrepasado, de modo que, conforme a lo expresado anteriormente, no puede concluirse que el ciberataque revistiera la naturaleza de

---

indiscriminados, definiendo los mismos como: "*a) los que no están dirigidos contra un objetivo militar concreto; b) los que emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o c) los que emplean métodos o medios de combate cuyos efectos no sea posible limitar conforme a lo exigido por el presente Protocolo; y que, en consecuencia, en cualquiera de tales casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil*. En su apartado 5 añade que se considerarán indiscriminados, entre otros, los siguientes tipos de ataque: "*a) los ataques por bombardeo, cualesquiera que sean los métodos o medios utilizados, que traten como objetivo militar único varios objetivos militares precisos y claramente separados situados en una ciudad, un pueblo, una aldea u otra zona en que haya concentración análoga de personas civiles o bienes de carácter civil; b) los ataques, cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista*".

329 GEISS, R. *Las estructuras asimétricas,* op. cit.; p. 14.

un ataque armado. No obstante, este supuesto puede servir de ejemplo, al tiempo que de advertencia, de futuros conflictos armados no internacionales, de carácter asimétrico, originados por ciberataques o, en el que los mismos se utilicen, como un método de combate. En estos casos, por lo tanto, la necesidad militar de esos ciberataques deberá ser probada por ambas Partes, sin perjuicio de su disparidad de capacidades.

Esta necesidad militar, íntimamente relacionada con la obligada distinción entre civiles y combatientes, que se verá posteriormente, rige con independencia de que el medio de combate, en cuestión, se halle, o no, expresamente prohibido por el DIH. Es decir, puede darse el caso de que el medio no esté prohibido, pero sí el modo en que éste se emplee, de forma que en su empleo regirá el sometimiento a la existencia de esa necesidad militar.

Además, el uso de internet como método de combate, presenta lo que podría considerarse una ventaja adicional, cual es la de poder distinguir claramente el objetivo al que va dirigido el ataque y eliminar, de esta forma, los llamados "daños colaterales", o, al menos, minimizarlos. En cualquier caso, será imprescindible ponderar la causación de daños y la ventaja militar que, de ello, se extraiga. Se trata, por lo tanto de una actividad a la que los Estados vienen obligados, por aplicación del DIH y que ha resultado ser obligatoria, cuando se ha planteado el uso de métodos de combate, que dificultan esta tarea, como es el caso de las armas nucleares[330]. En dicha ponderación o lo que es lo mismo, en cumplimiento de ese deber de proporcionalidad, será de aplicación el DIH consuetudinario, siempre teniendo en cuenta las circunstancias concretas del caso[331]. En consecuencia, serán, asimismo, de aplicación las normas 1, 6 y 7 de la Compilación de DIH consuetudinario, que también establecen la obligada distinción entre combatientes y personal civil, e imponen la evaluación previa de la necesidad militar del ataque[332].

330 Legality of the Threat or Use of Nuclear Weapons, doc. cit.; par. 95.
331 Supreme Court of Israel, Public Commitee against Torture in Israel v. Government of Israel, Case No. HCJ 769/02, 13 December 2006.
332 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario. Volumen I, op. cit.; pp. 1-8 y 22-33.

6.1.2. La distinción entre civiles y combatientes.

La obligación de distinguir entre objetivos civiles y militares, al objeto de que el combate se libre, exclusivamente, respecto de éstos últimos, aparece, expresamente, recogida en el artículo 52 del PA I[333].

Atendiendo a la definición que, por exclusión, se realiza en el referido artículo del PA I, los bienes resultan ser de naturaleza militar, en función del uso real o potencial, por parte del atacante, y no tanto en función de su naturaleza intrínseca. Por exclusión, también puede afirmarse que, todos los objetos que no estén, especialmente, protegidos pueden convertirse en objetivos militares[334].

Prácticamente de la misma forma se recoge esta definición en la Compilación de DIH Consuetudinario, cuya norma 8, determina que

> "Por lo que respecta a los bienes, los objetivos militares se limitan a aquellos bienes que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar y cuya destrucción total o parcial, captura o neutralización ofrezca, en las circunstancias del caso, una ventaja militar definida".

Esta norma resulta aplicable, tanto a los conflictos armados internacionales, como a los de carácter no internacional.

Así pues, ambos criterios, recogidos en el mencionado artículo 52 del PA I, han sido trasladados a la norma 8, de tal manera que, el ataque deberá cumplir con ambas condiciones: que el objeto del mismo, contribuya de forma efectiva a la acción militar contra el enemigo y, además que su destrucción, captura o neutralización ofrezca una ventaja militar definida para el atacante. Sin embargo, dado que ambos elementos han de juzgarse, en el momento preciso de la

333 El artículo 52 establece que «*Los bienes de carácter civil no serán objeto de ataques ni de represalias. Son bienes de carácter civil todos los bienes que no son objetivos militares en el sentido del párrafo 2. 2. Los ataques se limitarán estrictamente a los objetivos militares. En lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida. 3. En caso de duda acerca de si un bien que normalmente se dedica a fines civiles, tal como un lugar de culto, una casa u otra vivienda o una escuela, se utiliza para contribuir eficazmente a la acción militar, se presumirá que no se utiliza con tal fin*».

334 SASSÒLI M., BOUVIER A. A., QUINTIN, A. How does law protect in war?, op.cit. ; Cap. 9; pp.5 y 6.

determinación del objetivo militar, y que, ello ha de hacerse de conformidad con las circunstancias del caso, tampoco aquí puede evitarse el elemento subjetivo. Por ello, resulta de suma importancia tener presente la casuística precedente, a través de la que podrán perfilarse las limitaciones al uso de la fuerza.

En el caso de los ciberataques ello cobra una especial relevancia, habida cuenta la interconectividad de redes, así como la gestión que, de las redes de uso militar, realizan entidades civiles. En todo caso, no puede olvidarse que un ataque informático no impide, *per se*, realizar esta distinción. Antes bien, los casos que se han ido exponiendo demuestran la capacidad de los ciberatacantes para seleccionar sus objetivos, así como la duración y efectos de los ataques[335].

En este sentido, resulta indiferente que la obligación internacional que se incumple lo sea de acción o de resultado. En el supuesto de un ataque a las comunicaciones civiles, de un Estado en conflicto, podría suceder que no se consiguiera el éxito del ataque o el resultado perseguido, por contar dichas comunicaciones con una eficaz protección o resiliencia, frente a ataques informáticos, pero ello no impediría la calificación de la conducta, como una violación de una obligación internacional de DIH, al infringir la prohibición de distinguir bienes civiles y militares.

Por otra parte, el principio de distinción entre combatientes y no combatientes es un principio básico en la aplicación del DIH, de forma que, únicamente, los miembros de un Ejército regular, perteneciente a un Estado, están autorizados a usar la fuerza contra el enemigo. Así, habida cuenta que los propios combatientes han de distinguirse, a sí mismos, de quienes no lo son, podrá exigirse responsabilidad a quienes participen en los combates sin autorización[336].

---

335 Los efectos producidos por el virus se propagaron más allá de su objetivo. Así lo reflejan Farwell y Rohozinski: "*Stuxnet has apparently infected over 60,000 computers, more than half of them in Iran; other countries affected include India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland and Germany. The virus continues to spread and infect computer systems via the Internet, although its power to do damage is now limited by the availability of effective antidotes, and a built-in expiration date of 24 June 2012*". FARWELL. J.P. y ROHOZINSKI, R. Stuxnet and the Future of Cyber War. Survival: Global Politics and Strategy 53:1, February – March 2011; pp. 23-40, en particular, p.2.

336 Así se expresa tanto el DIH convencional como consuetudinario. En el primer caso, esta norma viene impuesta por el artículo 48 del PA I, que establece: "*A fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las Partes en conflicto harán distinción en*

Sin embargo, esta distinción, entre combatientes y no combatientes, se hará especialmente complicada en los casos de ciberataques, por la dificultad de identificar a los autores y de vincularlos a la acción de un Estado. Nos encontramos con un problema de difícil solución, como se puso de manifiesto en el año 2007 en Estonia, cuando los mismos ciudadanos, que manifestaban su protesta en las calles de Tallin, presumiblemente, organizaron los ataques informáticos, que dejaron bloqueadas las principales instituciones de Estonia durante días. En este caso, no existía ningún conflicto armado, pero en el supuesto de que, la situación se hubiese producido en un contexto bélico, como afirma HUGES, podría haberse exigido responsabilidad a los ciberatacantes, a la luz del DIH[337]. Abundando en el primero de los ejemplos, cabe realizar una reflexión, adicional, a la que aporta HUGES, por cuanto no sólo los atacantes resultaron ser, presumiblemente, civiles, sino que las víctimas del ataque, ciertamente, lo fueron. Nuevamente, el PA I, en su artículo 50, define a la población civil, de forma excluyente, como toda aquélla que no sea combatiente[338]. Ninguna duda cabría, no obstante, en entender que, algunos de los ciberataques recibidos por Georgia, durante el conflicto sostenido con Rusia, se sujetaron a las limitaciones aquí expresadas.

Consecuentemente, la población civil ha de quedar protegida de los ataques, salvo que dicha población pierda la protección, otorgada por su participación directa en los mismos, tal como expresa el artículo 53 del mismo PA I.

Esta distinción conlleva que la mera presencia de personal civil entre personal combatiente determine que, a toda la colectividad, le sea aplicada la referida protección, sin perjuicio de que el personal militar combatiente, en

---

todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares". Por su parte la Compilación de DIH consuetudinario, en su norma 1, expresamente recoge que "*Las partes en conflicto deberán distinguir en todo momento entre personas civiles y combatientes. Los ataques sólo podrán dirigirse contra combatientes. Los civiles no deben ser atacados*".

337 Así lo pone de manifiesto HUGES, R., en *A treaty for cyberspace,* op. cit.; p.537.

338 El referido artículo 50, en su apartado 1, establece: "*Es persona civil cualquiera que no pertenezca a una de las categorías de personas a que se refieren el artículo 4, A. 1), 2), 3), y 6), del III Convenio, y el artículo 43 del presente Protocolo. En caso de duda acerca de la condición de una persona, se la considerará como civil*".

cumplimiento de este principio de distinción, así como del de proporcionalidad, pueda ser atacado con las medidas que exija la situación concreta[339]. En el caso de que los ciberataques lanzados contra Estonia se hubieran producido durante un conflicto armado, resulta claro que, también, podría haberse exigido responsabilidad criminal, de conformidad con el DIH, por el lanzamiento de ataques cibernéticos a la población civil. En este caso, los ataques sufridos en las redes informáticas afectaron, casi en exclusiva, a la población civil negando a la misma el acceso a determinados servicios de distinta naturaleza y relevancia[340].

Resulta de suma importancia pues, deslindar quiénes pueden considerarse civiles en conflictos armados internos en los que se usen armas cibernéticas. Esta cuestión, indefectiblemente, conlleva una consideración adicional. Si bien otras armas que podríamos considerar convencionales, sólo se encuentran en poder de los Estados o bien son de difícil adquisición o de manejo imposible por la población civil (pensemos, por ejemplo, en armas nucleares o bombas de racimo), en el caso de internet, esto no ocurre. Muy al contrario, su mayor ventaja, como es un acceso prácticamente universal, al menos en el mundo desarrollado, se convierte aquí en un reto.

339 Al respecto, el artículo 50 del PA I, en su apartado 2 establece: "*La presencia entre la población civil de personas cuya condición no responda a la definición de persona civil no priva a esa población de su calidad de civil*".

340 Los objetivos atacados, con carácter principal, fueron páginas pertenecientes al Gobierno de Estonia y los ataques consistieron en la denegación de acceso a las mismas. También fueron atacados los canales habituales de información del Gobierno hacia el exterior, a través de internet. Asimismo, algunas instituciones privadas fueron objetivo de los ciberatacantes, de manera que la mayoría de los bancos de Estonia vieron interrumpida su actividad durante horas. El portal de internet del segundo banco comercial más importante del país, dejó de funcionar durante casi dos horas, sin poder, así, prestar servicio a sus clientes en Estonia durante ese tiempo y durante todavía más tiempo a aquellos que pretendían realizar sus actividades por internet desde fuera de Estonia. Los ciberatacantes llegaron a dañar la página web del Partido Reformista de Estonia, alterando su contenido y reemplazando la fotografía de su líder por otra en la que lucía una estética hitleriana. Igualmente, se comprobó el envío grandes cantidades de spam, es decir, de correo electrónico no deseado, enviado de forma tan masiva, que llega a saturar la cuenta de correo de quien lo recibe, hasta el punto de inutilizar la cuenta. Los objetivos seleccionados fueron de muy diversa entidad e incluyeron servicios, en algunos casos, críticos como el teléfono de emergencias 112, que por unos momentos quedó sin inoperativo. Las páginas web que, de una u otra forma, se vieron afectadas fueron las del Gobierno de Estonia, su Primer Ministro, el Presidente, el Parlamento, la mayoría de los Ministerios, así como instituciones estatales, como la Policía Nacional o el Partido Reformista. En el ámbito privado, la mayoría de los bancos que ofrecían un servicio on-line, se vieron afectados y también portales de noticias o redes de telefonía móvil. Lo mismo cabe decir de proveedores de servicio de internet. Así puede leerse en TIKK, E. KASKA, K, VIHUL, L., International Cyberincidents, op. cit.; pp.18-23.

Por otro lado, la participación directa en las hostilidades será igualmente de gran trascendencia, a pesar de las dificultades de índole técnica que pudieran darse. En un ataque cibernético, que pudiera considerarse ataque armado, se pondrá de manifiesto la dificultad de discernir, por una parte, su origen y, posteriormente, si el medio ha sido empleado, por parte de un Estado o, por un particular que actúe por cuenta propia, o como agente de un Estado, sea éste persona física o jurídica. Ciertamente, no constituye esto una tarea sencilla, como se verá a analizar la atribución del hecho ilícito al Estado, pero aun así, puede afirmarse, inicialmente, que hay algunas situaciones en las que el principio de distinción es aplicable de forma sencilla a los ciberataques, como el supuesto en que el objetivo es un sistema de control aéreo militar y el ataque ocasiona un accidente al transporte militar.

Asimismo, hay casos evidentes de ataques ilícitos, como los que podrían darse contra las redes de hospitales, museos y lugares especialmente protegidos, aun cuando ofrecieran ventaja militar. No obstante, el elemento cibernético influye directamente en cuestiones tales como, la naturaleza del personal implicado en su desarrollo, frente a quien, evidentemente, tendrá que regir el principio de distinción. Es decir, si tradicionalmente, la persona civil que diseña un arma no ha sido considerada un participante directo en las hostilidades, habrá que resolver la cuestión de si ese mismo estatuto puede y debe reconocerse al personal civil, encargado de descifrar determinados códigos o programas informáticos, respecto de quienes se considera alterado ese estatuto, pudiendo, así, ser objetivos lícitos en un contraataque[341].

Por último, hay que tener presente que la definición de cuáles sean objetivos militares no puede depender del medio o método de guerra utilizado. Por el contrario, el principio se aplicará, tanto a métodos y medios cinéticos, convencionales, como a los que no lo son, siendo indiferente, asimismo, que una operación cibernética cause o no la destrucción del objetivo atacado[342]. Sin

341 HATHAWAY, O. A. y otros. *The law of cyber-attack*, op. cit.; p.858.
342 CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos.* Informe resultante de la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, op.cit.; p. 42.

embargo, no puede soslayarse el hecho de que, este método de combate que se analiza, plantea interrogantes hasta ahora inéditos, como, por ejemplo, si los datos informáticos pueden tener la consideración de "objeto" a los efectos aquí expuestos, sin que su intangibilidad pueda privar, a priori, de tal consideración.[343]

Nuevamente, surge la cuestión, que más adelante se abordará, en relación a la atribución de la conducta a un Estado o agente del Estado, pues en este sentido, algunos autores entienden que, los criterios que han de aplicarse de conformidad con la ley para determinar cuál ha de ser el uso proporcionado de la fuerza, se establecen "*once a state or identifiable group-supported attack on the security of the nation has taken place*[344]".

Con independencia de estas posteriores cuestiones, es el momento de abordar una de las principales consecuencias de la violación de cualquiera de las obligaciones internacionales que aquí se exponen. Una vez cometido el hecho ilicto, a través de la violación de estas obligaciones, nace la responsabilidad internacional que, como afirma PÉREZ GONZÁLEZ, "*suele concretarse- aunque ello no excluya otras modalidades- en el deber de reparar*[345]". Por lo tanto, a la vista del especifico conteneido de la obligación violada, habrá que entrar a valorar el correlativo contenido de la relación jurídica de responsabilidad.

---

343 Otros autores, sin embargo, expresan una opinión opuesta, manifestándose en contra de la consideración de dichos datos, como objetivo: "*While there is no definitive answer to this question, the currently prevailing view among LOAC experts appears to hold that in most cases data, for the purposes of LOAC targeting, should not be considered an object*". Así puede leerse en, LUBELL, N. *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply*? International Law Studies. U.S. Naval War College. Volume 89, 2013; pp. 252-275, en particular, p. 267.

344 En el mismo sentido, TERRY entiende que "*No state is obliged to ignore an attack as irrelevant, and the imminent threat to the national security requires consideration of a response. One such lawful response is the elimination of the very computer infrastructure that allows the enemy's weapons systems to function*". TERRY, J. P., *The lawfulness of attacking computer networks in armed conflict and in selfdefense in periods short of armed conflict: what are the targeting constraints? The navy's EEO complaint pilot program*. Military Law Review, Vol.169. September 2001; pp.70-91, en particular; p.80.

345 Asimismo, el profesor PÉREZ GONZÁLEZ, pone de manifiesto que esta "*situación nueva en que consiste la responsabilidad internacional supone la concurrencia de dos situaciones jurídicas subjetivas: una activa, representada básicamente por el derecho subjetivo lesionado, que da pie al sujeto que sufre la lesión a reclamar y otra pasiva, representada por las nuevas obligaciones del sujeto responsable derivadas de la violación de la obligación impuesta por la norma primaria y que suelen concretarse en el deber de reparar (sin excluir por ello otras posibles expresiones de la responsabilidad*". PÉREZ GONZÁLEZ, M. *La responsabilidad internacional (I): el hecho internacionalmente ilícito*, op. cit.; pp. 873 y 874.

Este deber de reparar, sin embargo, no excluye la obligación de dar cumplimiento a la obligación, que ha sido infringida pues, en otro caso, podría constituirse en una suerte de justificación de la ilegalidad internacional. Antes bien, el primer deber, que se impone al Estado infractor, consiste en cesar en la infracción y cumplir con la obligación violada[346].

La obligación de cesación y de cumplimiento de la norma violada aparece recogida en el artículo 29 del Proyecto, que establece que: "*Las consecuencias jurídicas del hecho internacionalmente ilícito con arreglo a lo dispuesto en esta parte no afectan la continuidad del deber del Estado responsable de cumplir la obligación violada*".

Así, la violación de una norma de DIH en el transcurso del combate, implicara la obligación de reparar la infracción, a través de las medidas que más adelante van a ser estudiadas. Es decir, en el supuesto que aquí se presenta, en el que se ataca militarmente un objetivo civil, infringiendo así la obligación de distinguir entre bienes civiles y militares, el deber de cesar y cumplir con la obligación violada impone, en primer lugar, el cese del ciberataque que se estuviera produciendo. Si en un caso como este se hubiera atacado una página web de una empresa o de una entidad pública civil, la responsabilidad del Estado comenzará por cumplir con el deber de distinguir, con independencia, pues, de si se han producido o no daños materiales y, en su caso la cuantía de los mismos.

En este sentido se expresa el Proyecto, cuando, en su artículo artículo 30 establece que,

> "El Estado responsable del hecho internacionalmente ilícito está obligado:
>
> a) A ponerle fin si ese hecho continúa;
>
> b) A ofrecer seguridades y garantías adecuadas de no repetición, si las circunstancias lo exigen".

346 Tambíen el profesor PEREZ GONZALEZ afirma que "*En todo caso y, en lo concerniente al contenido de la responsabilidad, las consecuencias jurídicas que se producen en el contexto de esa relación nueva entre el Estado autor del hecho y otros Estados, no afectan a la continuidad del deber del Estado responsable de cumplir la obligación violada por él*"; *Ibidem*; p. 874.

La Jurisprudencia internacional, por su parte, también ha sido muy clarificadora a la hora de establecer los requisitos que hacen surgir el deber de cesación, exigiendo así, "*que el hecho ilícito tenga carácter continuo y que la norma violada siga en vigor en el momento en que se dicta esa providencia*[347]". Como ya se ha anticipado, el artículo 29 del Proyecto enuncia el principio general de que las consecuencias jurídicas de un hecho, internacionalmente ilícito, no afectan la continuidad del deber del Estado responsable, de cumplir la obligación violada, en tanto que sigue en vigor la relación jurídica preexistente. En consecuencia, ni siquiera en los supuestos en que el Estado procede a cesar el incumplimiento y repara el perjuicio, quedará exonerado del deber de cumplir con la obligación violada.

La continuidad del deber de cumplir con una obligación internacional, pese a su violación, está subyacente en el concepto de hecho ilícito continuado, previsto en el artículo 14 y en la obligación de cesación del artículo 30 del Proyecto, que enuncia las primigenias obligaciones, del Estado infractor: cesar en la infracción y repararla. Se trata, por lo tanto, de dos consecuencias inmediatas que pretenden "*poner fin al comportamiento ilícito que continúa, mientras que las seguridades y garantías cumplen una función preventiva y pueden describirse como un reforzamiento positivo del cumplimiento futuro*[348]".

Como puede deducirse del Comentario al Proyecto de artículos, la cesación cumplirá su objetivo, de forma más evidente, en los casos en que el ilícito esté constituido por un hecho continuado, de la índole de los ya examinados al analizar la necesidad de vigencia de la obligación violada. Sin embargo, el citado artículo 30 contempla, asimismo, los supuestos en que la violación se produce a través de hechos repetidos e independientes.

Podría darse la hipotética situación de que, infringiendo la norma de DIH que obliga a respetar a las personas y bienes civiles, se produjera un ciberataque a un banco privado. La importancia del sistema financiero, no debe ser infravalorada, pues ya se ha advertido que forma parte de uno de los sectores

347 Así puede leerse en el Comentario 3) al artículo 30 del Proyecto, al citar el fallo del caso *Rainbow Warrior*.
348 Comentario al artículo 30 del Proyecto.

que conforman las infraestructuras críticas. Pues bien, si un banco privado sufriera un ciberataque, por parte de las Fuerzas Armadas de la otra Parte beligerante, de modo que éstas dañaran su seguridad informática y, en consecuencia, su solvencia económica y reputación profesional, el sistema de reparación que prevé la Compilación de DIH, podría no ser suficiente. Si, como consecuencia del hecho anterior, los datos de los clientes de dicha entidad recalaran en manos de terceros, la responsabilidad internacional del Estado ejecutor de esa operación militar, sería tan indudable, como difícil de satisfacer.

La cesación del ciberataque a la entidad bancaria constituiría una primera e imprescindible medida, por cuanto supondría, en primer lugar, el restablecimiento de la legalidad internacional y, adicionalmente, la evitación de daños mayores.

La obligación de cesación adquiere, así, su mayor justificación al responder a situaciones como la descrita en que la violación de la obligación internacional se produce de forma continua y no será infrecuente, tratándose de ataques que se cometen a través de la red.

De la misma manera, el artículo 30 establece la obligación del Estado responsable consistente en "*ofrecer seguridades y garantías adecuadas de no repetición, si las circunstancias lo exigen*". Es decir, como el Comentario deja sentado, se trata de restablecer "*la confianza en una relación continuada, aunque suponen mucha más flexibilidad que la cesación y no se requieren en todos los casos*[349]".

En conclusión, tal y como asimismo afirma el citado documento, estas consecuencias "*pueden estar previstas en tales términos que se excluyan otras consecuencias, total o parcialmente*" pero "*a falta de una disposición específica, el derecho internacional atribuye al Estado responsable nuevas obligaciones, y en particular la obligación de reparar las consecuencias perjudiciales derivadas de ese hecho*[350]". Serán habituales estas seguridades y garantías en los casos en que el mero cese no suponga una satisfacción de la pretensión invocada por el Estado lesionado y,

349 Comentario al artículo 30 del Proyecto.
350 Comentario a la Segunda Parte del Proyecto.

también, cuando el restablecimiento de la situación inicial no queda suficientemente protegido.

El establecimiento de seguridades, tal y como prevé el Proyecto, podrá exigirse por el Estado perjudicado, pero si traemos a colación el contenido del artículo 48 del mismo, no podemos olvidar la posibilidad de que, cualquier Estado de la Comunidad Internacional protagonice tal solicitud, en los supuestos en que se viole una obligación que afecte a la Comunidad Internacional en su conjunto. Este supuesto resulta especialmente relevante en este ámbito que aquí se trata. Ya se ha apuntado el carácter de *ius cogens* que se puede predicar de determinadas normas que componen el DIH, sin perjuicio de que el análisis en profundidad de tal materia, se realice en el epígrafe correspondiente a las causas de exclusión de la ilicitud de la conducta.

En los supuestos en que la solicitud sea realizada, únicamente, por el Estado lesionado por la conducta ilícita, podrá conllevar, para el infractor, la adopción de comportamientos específicos. En el supuesto que aquí se contempla de forma hipotética, sería previsible que el Estado, en el que la entidad bancaria radica y de cuyas infraestructuras críticas forma parte, solicitara la adopción de medidas específicas encaminadas, por ejemplo, a evitar la evasión de la información.

En el caso, por ejemplo, del ataque al teléfono de emergencias sanitarias civiles que se produjo en Estonia, al que ya se ha hecho mención, podría suceder que el Estado lesionado solicitara la cesación del ataque y, además, la adopción de medidas de seguridad, tendentes a garantizar que dichos ataques no se volvieran a repetir, si dicho ataque se produjera, como consecuencia de la violación de una obligación de DIH durante el combate.

En el caso del ataque informático a la entidad bancaria, la reparación conllevará, necesariamente, la vuelta al estado del que se disfrutaba, con carácter previo al ataque. Pues bien, el propio Proyecto, al delimitar cuál sea este estado, especifica que no puede entenderse por tal el que se hubiera producido, en el actual momento, en el caso de que no se hubiera realizado el ataque. Es decir, el estado al que ha de pretenderse volver es la situación fáctica en que se

encontraba el Estado, en el momento justo anterior al comienzo de la violación de la obligación de DIH. En efecto, la reparación de la situación debería ser entendida, de manera que repusiera al Estado lesionado, en el lugar en que, realmente, se habría encontrado, en caso de no haber sufrido la violación de la obligación internacional.

Sin embargo, el criterio adoptado por el Proyecto resulta manifiestamente preferible, por cuanto, la acreditación de la situación que se hubiera dado, en la entidad bancaria que aquí se trae a título de ejemplo, en el caso de no haberse producido el ciberataque, implica la realización de una labor que entraña demasiadas incertidumbres, pues dicha situación sólo podría conocerse de un modo probable, pero nunca indubitado. El cumplimiento de las obligaciones jurídicas, a las que la violación de una obligación internacional compele, no puede verse adulterada por la inclusión de datos inciertos, o con la necesidad de valorar hipótesis de imposible acreditación. Se trata, en este ámbito, de restablecer la situación que nunca debió de perderse y, a la vez, de garantizar, como tantas veces se ha dicho, la legalidad internacional y, en consecuencia, la seguridad jurídica, de modo que ambos objetivos podrían verse comprometidos, en el caso de adoptar el criterio que también el Proyecto rechaza.

En cualquier caso, aun en el supuesto descrito en el Proyecto, la reparación ha de ser íntegra, en el sentido de que ha de cubrir la producción de todo perjuicio sufrido, cualquiera que sea la índole del mismo, es decir, material y moral. Esta integridad de satisfacción se ve limitada a los daños que se hayan producido realmente, de manera que la reparación se contempla en el Proyecto, de forma amplia pero no ilimitada y, en todo caso, tendente a eludir las situaciones de abuso, en las que pudiera incurrir el Estado lesionado.

Por otra parte, hay que señalar que la reparación de los perjuicios, que cause la violación de una obligación internacional, resulta obligatoria para el Estado responsable, con independencia de la licitud de su conducta en el Derecho interno[351]. Es decir, nos encontramos ante un precepto que señala la coherencia

351 Así puede leerse en el artículo 32 del Proyecto.

con la construcción jurídica, que permite dirimir cuándo se ha producido la violación de una obligación internacional. En ese caso, al establecer la infracción de dicha obligación, es irrelevante la licitud en Derecho interno de la conducta. Así, en paralelo, la construcción de la relación jurídica que surge de la violación, contempla la irrelevancia jurídica de la conducta en relación al Derecho interno. No podría ser de otro modo pues, de ser admitida aquí la exención, quedaría sin efecto la calificación jurídica realizada previamente respecto de la conducta ilícita.

El modo en que haya de procederse a reparar al Estado perjudicado, será cualquiera de los prevenidos en el artículo 34 del Proyecto que entiende que "*La reparación íntegra del perjuicio causado por el hecho internacionalmente ilícito adoptará la forma de restitución, de indemnización y de satisfacción, ya sea de manera única o combinada, de conformidad con las disposiciones del presente capítulo*".

En cualquier caso, habrá que tener en cuenta la advertencia realizada por el Comentario[352] cuando expresa la distinción entre la cesación y la reparación, aunque, puntualizando que la cesación no está limitada por la proporcionalidad.

6.1.3 La proporcionalidad del ataque.

La observancia de la proporcionalidad prohíbe el uso la fuerza, en un grado superior, al necesario para el cumplimiento del objetivo militar. En el caso de internet, podría considerarse que el uso de la red está sujeto a esta prohibición, por cuanto se trata de un método de combate que, efectivamente, podrá producir un daño indiscriminado, que afecte por igual a instituciones públicas y privadas, así como a civiles. Sentado lo anterior, la cuestión será determinar si la fuerza utilizada resulta proporcional al objetivo militar.

Si bien el principio de proporcionalidad se encuentra recogido en las normas de carácter convencional[353], los principios generales por los que se prohíbe el empleo de armas, que causan males superfluos o sufrimientos innecesarios, así como el empleo de armas de efectos indiscriminados, tienen

352 Comentario 7) al artículo 30 del Proyecto.
353 Este principio es el resultante de la aplicación de los artículos 35 y 57 del PA I.

naturaleza de normas de Derecho Consuetudinario aplicables en todo conflicto armado[354].

Con base, esencialmente, en estos principios, la práctica de los Estados ha conllevado la prohibición del empleo o ciertos tipos de empleos de diversas de armas específicas, a saber: las toxinas o armas tóxicas, las armas biológicas, las armas químicas, las sustancias antidisturbios como método de guerra o los herbicidas como método de guerra, entre otras[355]. Otras armas, que no están prohibidas como tales, se encuentran, de todos modos, sujetas a restricciones, tal y como ocurre con las minas antipersona y las armas incendiarias sin que, hasta la fecha, ninguna previsión específica se ha realizado sobre el uso de internet, como medio de combate.

El de la proporcionalidad ha sido uno de los principios más debatidos, por la doctrina contemporánea, a la hora de esclarecer la aplicación del DIH al medio de combate cibernético. Teniendo en cuenta el medio tan difuso en el que nos encontramos, resulta difícil concretar no sólo la proporcionalidad de un ciberataque, sino también la respuesta que pudiera darse en legítima defensa[356].

El principio de la proporcionalidad ha tenido su correspondiente reflejo en el ámbito del DIH Consuetudinario, que prohíbe el empleo de "*medios y métodos de guerra de tal índole que causen males superfluos o sufrimientos innecesarios*"[357]. La práctica de los Estados establece esta regla como una norma de Derecho Internacional Consuetudinario aplicable, tanto en los conflictos armados internacionales, como en los no internacionales. La CIJ, en su Opinión Consultiva relativa al uso de armas nucleares, declaró que, la prohibición de emplear medios y métodos de guerra, de tal índole que causasen males superfluos o sufrimientos

354 Así puede leerse en HENCKAERTS, J.-M., *Estudio sobre el derecho internacional humanitario consuetudinario: una contribución a la comprensión y al respeto del derecho de los conflictos armados.* Separata de la Revista Internacional de la Cruz Roja, vol. 87, núm. 857. Marzo 2005; pp. 1-50, en particular, p. 22.

355 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; pp. 281-340.

356 Así se expresa ANTOLIN-JENKINS, V. M., *Defining the parameters of cyberwar operations: looking for law in all the wrong places?* Naval Law Review 51, 2005; pp.132-174, en particular, p. 134.

357 Este principio se encuentra recogido en la Norma 70 de la Compilación de DIH Consuetudinario. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p.265-273.

innecesarios, constituye uno de los "*principios cardinales*" del DIH[358]. La Corte declaró, asimismo, que esta práctica es conforme con la aplicabilidad de la norma, tanto en los conflictos internacionales como en los no internacionales, ya que, en general, los Estados no disponen de armamentos militares diferentes para ambos tipos de conflictos.

Por lo tanto, nos encontramos ante una norma cuya aplicación no debería suscitar dudas, en casos análogos a los hasta ahora descritos, cuando la existencia de un conflicto internacional sea clara, con independencia del alcance que, en su momento, se otorgue a una eventual "declaración de guerra" como la emitida por Georgia en su día.

En tal caso, la prohibición de medios de guerra, de tal índole que causen males superfluos o sufrimientos innecesarios, se refiere a los efectos de un arma, sobre los combatientes. Aunque existe acuerdo general sobre la existencia de esta norma, las opiniones difieren, en cuanto al modo de determinar si un arma causa males superfluos o sufrimientos innecesarios En general, los Estados coinciden en que, todo sufrimiento que no tenga un fin militar, infringe esta norma[359]. En el caso de los males que se causaron a Estonia y también a Georgia, al margen de los que sufrió su Ejército, no cabe duda de que, la mayoría de ellos, entrarían dentro de la aseveración anterior. Efectivamente, muchos de los ataques sufridos por ambos Estados carecían de un objetivo militar y, además, tuvieron entidad suficiente para causar daños de ese tipo[360] .

358 Legality of the Threat or Use of Nuclear Weapons, doc. cit.; par. 78.

359 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; p. 268.

360 La página web del Parlamento de Georgia y la de la Presidencia del Gobierno sufrieron sendos ataques. Las websites de algunos Ministerios incluido el de Asuntos Exteriores dejaron dar servicio, así como algunas páginas comerciales. Además de las websites anteriormente mencionadas, cabe añadir la del Banco Nacional de Georgia, las páginas de algunas agencias de noticias. También la página oficial del Gobierno de Abjasia fue atacada, así como la del Ministerio de Educación y Ciencia de Georgia; foros de opinión; la web de la Asociación de la Prensa; de compañías de televisión; y de portales de noticias, entre otras. En el caso de Estonia, la Administración se vio imposibilitada en su funcionamiento y comunicación con los ciudadanos, la banca no pudo operar durante días, se impidió dar información al exterior de lo que estaba ocurriendo en el país y servicios básicos como el teléfono de emergencias 112 quedo bloqueado durante horas. TIKK, E. KASKA, K., RÜNNIMERI, K., KERT, M., TALIHÄRM, A.-M., VIHUL, L. Cyber Attacks Against Georgia, op. cit.; pp. 4-17.

En directa conexión, con el principio antes visto de la necesidad militar, la norma exige la existencia de un equilibrio entre ésta y los daños previstos o los sufrimientos infligidos a las personas. De forma que esos daños o sufrimientos excesivos, es decir, desproporcionados con respecto a la ventaja militar prevista, transgreden la norma 70 de la Compilación de DIH Consuetudinario. La CIJ, en la referida Opinión Consultiva, definió sufrimiento innecesario como "*un sufrimiento superior al daño inevitable para alcanzar objetivos militares legítimos*"[361]. Un factor importante a la hora de establecer si un arma puede causar males superfluos o sufrimientos innecesarios es que no pueda evitarse una discapacidad grave permanente, lo que queda inmediatamente relacionado con el empleo de aquellas armas que causan inevitablemente la muerte. Ciertamente, no fue éste el caso de los ciberataques aquí analizados, pero esto no puede impedir la aplicación de la norma a aquéllos que, en un futuro, se demuestren capaces de serlo. En principio, no puede descartarse que, a través de un ataque informático, se dañen las infraestructuras críticas de un Estado impidiendo a la población el acceso a recursos vitales.

En los supuestos considerados no se produjo un efecto de devastación permanente sino que, como la mayoría de los ataques informáticos, éstos tuvieron una duración limitada en el tiempo y, pasado el momento del ataque, sus efectos no permanecieron. Sin embargo, hay que tener presente que la interrupción del servicio de internet se produjo, para Georgia, en el momento en que este país se encontraba más vulnerable, por hallarse inmerso en una situación de conflicto armado. Prueba de ello es que se privó, al Estado, de su posibilidad de uso de internet, cuando el empleo de las comunicaciones se presentaba como crucial. En este contexto, la falta de información podría haber originado la adopción de decisiones, por parte del Gobierno de Georgia, en un sentido distinto del que hubiera resultado, en el caso de contar con información, actualizada en cada momento.

Ni en Estonia ni en Georgia los daños materiales, ni tampoco los de carácter personal, parece que fueran de la suficiente entidad, como para

361 Legality of the Threat or Use of Nuclear Weapons, doc. cit.; par.78.

considerarlos equiparables a los que se producen por un ataque armado convencional.

Por otra parte, también la práctica de los Estados ha logrado que quede prohibido el empleo de armas, de tal índole que sus efectos sean indiscriminados" [362]. En el ámbito que ahora se examina, podría darse la propagación de un virus informático en los sistemas de un determinado Estado, elegido como objetivo. Cabría, asimismo, la posibilidad de que se introdujera, únicamente, en la red militar de ese Estado, pero si ese virus resultara altamente pernicioso podría contagiar los sistemas civiles e, incluso, propagarse más allá de las fronteras y perturbar o destruir la infraestructura, que depende de ellos. En este supuesto, nos encontraríamos ante un ataque indiscriminado, de conformidad con el DIH, siempre que se demostrara la imposibilidad de dirigir ese virus contra un objetivo militar concreto. De este modo, estaríamos expuestos a un método de combate cuyos efectos no pueden ser limitados, tal como lo exige el DIH[363].

La principal cuestión radica, pues, en conocer si el ciberataque puede dirigirse contra un objetivo militar y si es posible limitar sus efectos, como exige el DIH. Ambos elementos son los que requiere el artículo 51. 4 del PA I, en sus apartados b) y c). En efecto, internet, considerado como un medio de combate, podría hacer frente a las limitaciones que, en cuanto al uso de dichos métodos, imponen el DIH convencional y consuetudinario, por cuanto, a través de un ciberataque, se ha demostrado la posibilidad de elegir el objetivo de una manera clara y concreta. Esa concreción se demuestra en el objetivo elegido, en el momento de realizarlo, en el momento de su finalización, así como en los efectos a conseguir. Todo ello puede planearse, como de hecho así se hizo, en los sucesos ocurridos en Estonia, Lituania y Georgia, de modo que los ciberataques no quedarían incluidos *per se* en la definición de armas prohibidas. No obstante, no

362 Así puede leerse en la Norma 71 de la Compilación de DIH Consuetudinario. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, doc. cit.; pp. 273-279.

363 De este modo quedó expresada la aplicación de esta norma de DIH Consuetudinario al ámbito cibernético por CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*. Informe resultante de la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, doc. cit.; p. 42.

podría decirse lo mismo del "modo" en que ese arma sea utilizada. Al margen de que se haya venido utilizando de un modo que podríamos calificar de "*calculadamente controlado*", en principio, nada impide que a través de internet se produzca un ataque indiscriminado[364].

Si por el contrario deducimos que, sólo cuando un Convenio o la práctica internacional han prohibido el uso de un arma, puede entenderse que ésta se califica como prohibida, nos encontramos aún lejos de que esto sea así, con las operaciones cibernéticas. En este sentido, la Asamblea General de Naciones Unidas ha realizado una incipiente aproximación a este problema. Las Resoluciones emanadas en este ámbito, tienen como objetivo, principalmente, garantizar la seguridad en las comunicaciones por internet, pero todavía no contamos con ningún texto, que analice la licitud o ilicitud de este medio de comunicación usado como arma de guerra.[365]

---

364 Ha de recordarse, en este sentido que, como se ponía de manifiesto en el Capitulo Primero de este trabajo, aunque los efectos del virus Stuxnet no pueden ser calificados como indiscriminados, sí sobrepasaron su objetivo.

365 Desde el año 1998, Naciones Unidas, ha publicado una serie de resoluciones, entre las que cabe destacar, por una parte, la Resolución 55/63, de 4 de diciembre de 2000 y la 56/121, de 19 de diciembre de 2001, ambas, relativas a la lucha contra la utilización de la tecnología de la información con fines delictivos. Resolución 55/63 aprobada por la Asamblea General en su 81ª sesión plenaria, de 22 de enero de 2001. Doc. A/RES/55/63 y Resolución 56/121, aprobada por la Asamblea General en su 88ª sesión plenaria, de 23 de enero de 2002. Doc. A/RES/56/121. Asimismo, cabe citar la Resolución 57/239, de 20 de diciembre de 2002, relativa a la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales. Resolución 57/239, aprobada por la Asamblea General en su 78ª sesión plenaria, de 20 de diciembre de 2002.Doc. A/RES/57/239. Además, cabe mencionar que otro grupo de Resoluciones (Resolución 53/70, de a de diciembre de 1998, 56/19 de 29 de noviembre de 2001, 58/32, de 8 de diciembre de 2003, 62/17 de 5 de diciembre de 2007), relativas a los avances con respecto a las tecnologías de la información en el contexto de la seguridad internacional, estaban vigentes en el momento de producirse los hechos. Resolución 53/70, aprobada por la Asamblea General en su 79ª sesión plenaria de 4 de diciembre de 1998. Doc. A/RES/53/70; Resolución 56/19, aprobada por la Asamblea General en su 68ª sesión plenaria, de 19 de noviembre de 2001. Doc. A/RES/56/19; Resolución 58/32, aprobada por la Asamblea General en su 71ª sesión plenaria de 8 de diciembre de 2003. Doc. A/RES/58/32 y Resolución 62/17, aprobada por la Asamblea General en su 61ª sesión plenaria de 5 de diciembre de 2007. Doc. A/RES/62/17. La culminación a este proceso, viene dada por la Resolución de la Asamblea General 64/211 relativa a la creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales. En la misma, se incide nuevamente en la preocupación por las amenazas para el funcionamiento fiable de las infraestructuras de información esenciales y la integridad de la información transmitida por estas redes, en tanto puedan afectar al bienestar interno e internacional. Se exhorta en este ámbito a una colaboración a nivel internacional, a fin de afrontar de modo efectivo el carácter cada vez más transacional de estas amenazas. Resolución 64/211 aprobada por la Asamblea General en su 66ª sesión plenaria de 21 de diciembre de 2009. Doc. A/RES/64/211. Recientemente, ha sido creado

Una cuestión particular que surge y que requiere atenta reflexión es si, en la práctica, es posible anticipar, totalmente, las consecuencias o los efectos secundarios, que un ataque dirigido contra un objetivo militar legítimo, pueda tener en la población civil y los objetos de carácter civil. En este caso es necesario, igualmente, respetar los principios de distinción y proporcionalidad. Esto, a su vez, implica que es indispensable tomar algunas precauciones en el ataque. Estas precauciones, no son otras distintas a las que están contempladas en el artículo 57 del PA I, de forma que el autor del ataque tome todas las precauciones que sean factibles, al seleccionar los medios y métodos de ataque, con miras a evitar y, en cualquier caso, a reducir al mínimo las víctimas y los daños civiles incidentales. Es aquí donde puede obtenerse una mayor ventaja del empleo de los medios cibernéticos, por cuanto, en determinados casos las operaciones cibernéticas podrán causar un número menor de víctimas y daños civiles incidentales, en comparación con los que ocasionan las armas convencionales. En tales supuestos, el Estado o agente que actúe en su nombre, tendrá que considerar la posibilidad de lograr la misma ventaja militar, utilizando un método de combate cibernético.

Por ejemplo, un ciberataque que, de forma efectiva, paralizase la transmisión de información a través de internet podría, someramente, molestar a la población, pero, también, podría tener la capacidad suficiente, como para originar que los hospitales no pudieran comunicar información vital y, en definitiva, llegar a ocasionar la pérdida de vidas humanas. El principio de proporcionalidad, por lo tanto, obliga a considerar, anticipadamente, las consecuencias probables de una acción. Esta labor se presentara complicada, cuando no imposible, en el contexto de una ciberguerra, por lo que los ciberataques pueden, también, variar la importancia que se otorgue a las consecuencias temporales o no letales[366].

---

un Grupo de Expertos para el análisis de estas cuestiones. Como resultado del trabajo de dicho Grupo, puede destacarse el Informe emitido en Julio de 2015. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General. Seventieth sesión. Doc. A/70/174.

366 HATHAWAY, O. A. y otros. *The law of cyber-attack*, op. cit.; p. 855.

En este contexto, la conducta del Mando militar resulta esencial porque, como pone de manifiesto FENRICK a este Mando será a quien, en la planificación de la operación correspondiente, le sea exigible la «*responsabilidad de tomar todas las medidas necesarias para evitar daños a la población y bienes civiles*».[367]

Por otra parte, no puede desatenderse la estrecha relación entre la obligación que aquí se examina y, la que ya ha sido analizada, en relación con la distinción entre bienes y personas de carácter civil, pues la regla de la proporcionalidad ha sido entendida como una manifestación de esa obligación de distinción, sin la que la anterior, no podrá darse por cumplida[368].

Una vez acreditada la responsabilidad internacional del Estado, como consecuencia de la violación de esta obligación internacional, surgirá, como se veía en el supuesto anterior, la consiguiente obligación de reparar. Si durante el combate, a través de un ciberataque, se hubieran causado daños desproporcionados o sufrimientos innecesarios, la producción de daños implicará, asimismo, la elección de un medio de reparación, adecuado, para el restablecimiento de la situación. Esta valoración deberá hacerse desde un punto de vista material o económico, pero la misma no evitará la necesidad de cesar en el incumplimiento. Antes bien, esto constituye un simple comienzo, a partir del que los modos de reparar encontrarán muy diversas manifestaciones.

---

367 El autor, en este sentido entiende que "*Commanders and planners will be required to determine the relative weights of military advantage and civilian losses to determine if losses are excessive. "Excessive" is undefined and probably undefinable but frequent practice in deciding on the issue will probably result in the development of a "reasonable officer" view of the standard*". FENRICK, W.J. The rule of proportionality and Protocol I in conventional warfare. Military Law Review.Vol. 98, Fall 198; pp. 91-127, en particular, p. 128.

368 Asi lo pone de manifiesto RICHARDSON, quien al respecto argumenta que "*An important extrapolation of the principle of distinction is the principle of proportionality, whereby – when lawful targets are attacked – collateral damage to civilians/civilian objects must not be expected to be 'excessive' compared with the military advantage anticipated.*" Por otra parte, analizando, en concreto, las operaciones cibernéticas, en este caso, CNA, RICHARDSON advierte de que "*Feasible precautions must be taken prior to any attack, including a CNA. When a civilian is engaged in any form in a CNA, the act constitutes direct participation in hostilities and the actor loses civilian protection from attack. In modern warfare, distinction has become problematic due to the growing pervasiveness of 'dual-use' infrastructure. For instance, a power plant may serve a military function such as providing electricity to a military base or a munitions plant, which are both likely to be deemed legitimate military objectives. However, it may also be the sole source of electricity for the civilian population, powering hospitals, water treatment plants, and transportation*". RICHARDSON, J. *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, 29 J. Marshall J. Computer*. Journal of Computer & Information Law, vol. 29, issue 1. Fall 2011; pp. 1-29, en particular, p. 11.

Es decir, además de que, el Estado infractor esté obligado a cesar en la violación de la obligación internacional y a cumplir con la misma, adicionalmente, el Proyecto establece una serie de medidas tendentes a hacer efectiva la obligación de reparar. El mecanismo que el Proyecto prevé constituye un método de desagravio que se articula de forma priorizada, de forma tal que los mecanismos ulteriores únicamente entrarán en juego, a falta de efectividad de los precedentes.

Así, en primer lugar, la responsabilidad internacional ha de ser satisfecha a través de la restitución, es decir, la reposición al Estado perjudicado, en la situación previa a la infracción.

La reparación del daño, que contempla el Proyecto, queda encabezada por este modo de actuación que, asimismo, se recoge en la tan citada Compilación de DIH consuetudinario cuya aplicación, nuevamente, habrá que contemplar. En este ámbito concreto, la Compilación de DIH consuetudinario, una vez más, recoge la literalidad de las prevenciones contenidas en el Proyecto e indica que, el propósito de la restitución consiste en el restablecimiento de la situación existente, con carácter previo, a que se cometiera el hecho ilícito.

Por su parte, el Proyecto, en su artículo 35, aborda el modo de llevar a cabo la restitución, teniendo en cuenta, para ello, dos limitaciones que, en el caso de los ciberataques, cobran gran relevancia. En primer lugar, entiende el Proyecto que la restitución ha de procurarse siempre que "[no] *sea materialmente imposible*". Esta limitación será invocada en todos los supuestos en que se produzcan daños irreversibles, como los que antes han sido apuntados.

El uso de internet como método de guerra exige, nuevamente, examinar una serie de peculiaridades de ejecución, muy específicas de este método. Asimismo, también habrá que tener en cuenta el efecto multiplicador que puede alcanzar un ciberataque. Es decir, la infectación de un equipo informático puede producir, en muy poco tiempo, la propagación del virus de que se trate. Ello tendrá consecuencias a la hora de analizar si el ciberataque ha sido diseñado y lanzado, conforme a las limitaciones que ya han sido analizadas a lo largo del presente estudio. Pero, además, tendrá que tenerse presente este aspecto, a la

hora de exigir la responsabilidad, que aquí se estudia pues, evidentemente, en determinadas ocasiones, el lanzamiento de un ciberataque conllevará la pérdida del control de su ejecución y efectos, en poco tiempo.

En segundo lugar, el mismo artículo establece otra limitación a la obligación de restituir, que se halla estrechamente relacionada con la obligación que aquí se trata, pues el citado artículo establece que la reparación ha de hacerse de forma que no "*entrañe una carga totalmente desproporcionada con relación al beneficio que derivaría de la restitución en vez de la indemnización*".

En el específico ámbito del DIH, hay que acudir, nuevamente, la Compilación de DIH Consuetudinario que recoge los preceptos que, de forma expresa, prevén la restitución en el caso de violación de estas normas. El Comentario que acompaña a la exposición de la norma 150 de la Compilación relaciona la obligación de restituir, contenida en el articulo 35 del Proyecto, con la prevista en el "*párrafo 1 del primer Protocolo de la Convención de La Haya para la protección de los bienes culturales se establece que los Estados deben impedir la exportación de bienes culturales de territorios ocupados*[369]".

Por su parte, el mismo texto recuerda que el párrafo 3, del mismo Protocolo, obliga al Estado "*ocupante a devolver los bienes culturales exportados en violación del párrafo 1 al término de las hostilidades en el territorio previamente ocupado*". Pues bien, de nuevo la literalidad de los preceptos se presenta escasa para dar respuesta a todas las situaciones que podrán presentarse, en relación a la violación de las normas de DIH, a través de ciberataques cuando los mismos resulten desproporcionados. En los supuestos que recoge la Compilación es evidente que la restitución es posible y que cumple sus objetivos, sin embargo, retomando en el caso de un ataque cibernético desproporcionado, la limitación del texto, a la hora de determinar cual ha de ser la acción restitutoria, es evidente.[370].

---

369 Así aparece recogido en el Comentario a la Norma 150 de la Compilacion. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; p. 608.

370 El comentario al artículo 35 recoge las distintas acepciones del concepto de restitución y afirma que, en función de una de ellas, la restitución consiste en "*restablecer el statu qua ante, a saber, la situación que existía con anterioridad a la ocurrencia del hecho ilícito. De acuerdo con otra*

La restitución de bienes se presenta, así, como el paradigma de esta institución jurídica[371]. Sin embargo, cuando la violación de una norma de DIH, en el desarrollo del combate se produzca utilizando internet, será también habitual la necesidad de restablecer situaciones económicas y aun jurídicas.

En el Comentario del Proyecto se citan situaciones de restitución, tales como la liberación de personas detenidas ilícitamente o la devolución de bienes confiscados ilícitamente pero, asimismo, se admite la posibilidad de tener que acudir a "*un acto mucho mas complejo*", sin olvidar que "*la restitución es la principal forma de reparación*".

En el caso que antes se proponía, por ejemplo, el Estado infractor debería ser obligado a restablecer la seguridad de la entidad bancaria y la indemnidad de sus clientes; hechos ambos que, a buen seguro, necesitarían de la ejecución de medidas adicionales. Estas actuaciones no quedan al margen de la relación jurídica de responsabilidad, sino que forman parte del contenido de la misma, pues el Estado, declarado responsable estaría "*obligado a borrar todas las consecuencias jurídicas y materiales de su hecho ilícito mediante el restablecimiento de la situación que habría existido de no haberse cometido este hecho*[372]".

Con la exposición del caso que se ofrece a título de ejemplo, se pretende enfatizar en las peculiaridades que presenta el uso del medio cibernético en el combate y las consecuencias que tendrá el incumplimiento de dichas normas. Estas consecuencias se reflejarán, igualmente, en la reparación de los perjuicios causados, por la violación de las normas del combate. En el uso de cualquier otro método de combate o, en la reparación de las consecuencias producidas por la violación de otras normas, la restitución se producirá de modo natural, sin

---

definición, la restitución es el establecimiento o restablecimiento de la situación que habría existido de no haberse cometido el hecho ilícito. La primera definición es la definición estricta; no abarca la compensación que puede deberse a la parte lesionada por la pérdida sufrida, por ejemplo, por la privación de uso de los bienes retenidos ilícitamente pero ulteriormente devueltos. La segunda definición subsume en el concepto de restitución otros elementos de reparación íntegra y tiende a refundir la restitución como forma de reparación en la propia obligación básica de reparar.". Comentario 2) al articulo 35 del proyecto.

371 Así puede comprobarse a través del examen de la Norma 150 de la Compilación de DIH, que enuncia diversos casos en relación a los que se ha pronunciado la Jurisprudencia internacional. HENCKAERTS J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; p. 600.

372 Comentario 3) al artículo 35 del Proyecto.

perjuicio de la imposibilidad material de realizarla, basada en la destrucción o modificación de su naturaleza[373]. Sin embargo, aquí es preciso añadir las peculiaridades propias del método informático, que incluyen, entre otras, la puesta en evidencia de las vulnerabilidades de la red. Ello, a su vez, conllevará el descrédito en determinados sectores estratégicos, así como con la posibilidad de que, dicha manifestación pudiera ser objeto de provecho, por agentes no estatales, que pudieran, así, intervenir en el conflicto.

Se trata, por lo tanto, en este ámbito, de determinar la aplicabilidad de las formas de reparación previstas en el Proyecto, en los casos en que el Estado sea declarado responsable de violar la norma de DIH que impide la causacion de resultados desproporcionados. En este punto, pues, nada impedirá que se ejerza el derecho de restitución, pero teniendo en cuenta que, previsiblemente, será necesario abogar por otras medidas, que resulten más adecuadas a la naturaleza del perjuicio causado.

Por otra parte, la reparación consistente en la restitución, admite cualquier modalidad, que permita lograr el objetivo a alcanzar. Esta consideración, tradicionalmente, ha sido entendida en un sentido amplio, tal y como apunta el Comentario del Proyecto, que, incluso, prevé la llamada "*restitución jurídica*". Esta restitucion sera aquélla consistente en "*la modificación de una situación jurídica, bien en el marco del ordenamiento jurídico del Estado responsable, bien en el marco de sus relaciones jurídicas con el Estado lesionado*". De este modo, podrá ocurrir que, como consecuencia de la violación de una obligación internacional, se produzca un cambio jurídico, como los que el Comentario cita a título de ejemplo[374].

Por consiguiente, el término "restitución" puede comprender cualquier medida que resulte necesaria para "*corregir la situación resultante de su hecho*

373 Asi lo prevé el Comentario al articulo 35 del Proyecto, en su párrafo 4, cuando afirma que la posibilidad de restitución puede quedar excluida en la práctica, por ejemplo, porque los bienes de que se trata han sido destruidos o se ha modificado fundamentalmente su naturaleza, o porque por algún motivo no se puede reponer el *statu quo* anterior.

374 El Comentario al artículo 35, asimismo, señala que "*Estos casos comprenden la revocación, la anulación o la enmienda de una disposición constitucional o legislativa promulgada en violación de una norma de derecho internacional, la anulación o revisión de un acto administrativo, o de una resolución judicial ilícitamente adoptados, con respecto a la persona o bienes de un extranjero, o la exigencia de que se adopten disposiciones para dar por terminado un tratado*."Comentario 5) al articulo 35 del Proyecto.

internacionalmente ilícito", aunque esta afirmacion no puede interpretarse en el sentido de que la restitución de la legalidad vigente y, de la situación fáctica, sean ilimitadas. Antes bien, el Comentario admite que no existe obligación de restituir si la restitución "*entrañ[a] una carga totalmente desproporcionada con relación al beneficio que se derivaría de la restitución en vez de la indemnización*". Es decir, en el supuesto que se viene examinando a título de ejemplo, la rehabilitación del sistema informático de la entidad bancaria, la de su seguridad informática, así como la estimación del perjuicio causado a los clientes, los proveedores y los socios de la misma, conllevaría una serie de acciones, tan heterogéneas y complejas que, con toda probabilidad, podría invocarse la desproporción en relación al beneficio. En estos supuestos será necesario acudir al principio de equidad y a la buena fe, en orden a evitar situaciones, que pudieran resultar abusivas.

La Norma 150 de la Compilación de DIH Consuetudinario prevé, literalmente, que "*El Estado responsable de violaciones del derecho internacional humanitario está obligado a reparar íntegramente la pérdida o la lesión causada*". No se trata de una Norma específica, que excluya la aplicación de los artículos del Proyecto sino, antes bien, una confirmación del contenido del mismo.

Como advierte la citada Compilación, la obligación de reaparar se halla implícita en la norma de los Convenios de Ginebra que estipula que los Estados no pueden exonerarse, ni exonerar a otra Parte Contratante, de las responsabilidades en las que hayan incurrido a causa de infracciones graves[375].

Sin embargo, la reparación de los daños ocasionados, como consecuencia de la contravención de las mismas normas, en el lanzamiento de ciberataques sera dificil porque se producirán daños, en equipos o sistemas, que hayan sido infectados o inutilizados, como consecuencia de ciberataques masivos. También podrá darse la situación de una pérdida de información o de datos. En estos específicos supuestos, no parece que la reparación deba limitarse a restituir los bienes dañados. La reparación de daños inmateriales como los que, en numerosas

375 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; p.607.

ocasiones, se producirán como consecuencia de los ciberataques, va a resultar de difícil cumplimiento.

Así pues, la Compilación arroja escasa luz, sobre el modo en que haya de ser llevada a cabo esta tarea, ya que se limita a remitir al sistema general de responsabilidad internacional del Estado, previsto en el artículo 31 del Proyecto y de este modo entiende que, "*La reparación integra del perjuicio causado por el hecho internacionalmente ilícito adoptará la forma de restitución, de indemnización y de satisfacción, ya sea de manera única o combinada.*[376]"

En efecto, el artículo 31 establece que:

> "1. El Estado responsable está obligado a reparar íntegramente el perjuicio causado por el hecho internacionalmente ilícito.
> 2. El perjuicio comprende todo daño, tanto material como moral, causado por el hecho internacionalmente ilícito del Estado".

Es decir, se trata de que las consecuencias del hecho ilícito desaparezcan y el Estado agraviado pueda volver a disfrutar de la situación preexistente[377].

En consecuencia, la obligación de reparar no depende de la solicitud que formule un Estado, sino que es la consecuencia jurídica, automática, nacida de la comisión de un hecho internacionalmente ilícito.

La noción de "perjuicio", definida en el párrafo 2, incluye todo daño material o moral causado, aunque excluye las reclamaciones, meramente abstractas o los intereses generales de un Estado, que, individualmente, no ha resultado afectado por la violación. Según el Comentario, el daño "material" se refiere al daño a los bienes u otros intereses del Estado o sus nacionales que puede cuantificarse en términos financieros. En el ejemplo que antes se exponía, ese daño material, evidentemente estaría compuesto por la sustracción efectiva de dinero, la pérdida de contratos con socios y clientes o la disminución del valor de las acciones en bolsa, entre otros. El daño "moral", por contra,

376 *Ibidem*; p.607.
377 Comentario 2) al artículo 31 del Proyecto, citando el fallo relativo a la fábrica de Chorzow, Factory at Chorzow, doc. cit.; p. 47.

comprende hechos tales como, el dolor y el sufrimiento individuales, la pérdida de personas queridas o, la ofensa personal, asociada con la intrusión en el hogar o, la vida privada de una persona. En el ejemplo antes expuesto, consistiría básicamente en el descrédito de la entidad.

En el ámbito del DIH, la Compilación de DIH Consuetudinario cita expresamente, la necesidad de la "*restitutio in integrum*", consignada en el Proyecto[378]. Por otra parte, la propia naturaleza del origen de la obligación impide, en determinados casos, el reconocimiento de su existencia, como es el supuesto de los conflictos armados no internacionales. Es decir, si bien hasta ahora, se ha afirmado que la vigencia de las obligaciones de DIH resulta indiscutible también para los conflictos armados no internacionales, sin embargo, no puede decirse lo mismo del surgimiento de responsabilidad en el caso de violación de dichas normas, pues "*en los conflictos armados no internacionales las victimas sufren violaciones en su propio país y, en general, tienen acceso a los tribunales nacionales para reclamar una reparación con arreglo al ordenamiento jurídico interno.*[379]"

La restitución se dará siempre que sea materialmente posible y, siempre, teniendo en cuenta los derechos de terceros. Es decir, que si en el ejemplo anterior, el dinero sustraído resulta irrecuperable, la restitución será imposible. Si los datos del banco se han vendido y, con ello, se han originado transacciones de las que resultan terceros favorecidos, no podrán verse perjudicados por la reparación, pues no podrían resolverse negocios que ya se han celebrado.

El apartado b) del artículo 35 del Proyecto, también excluye la restitución si es completamente desproporcionada con la ventaja que podría obtener la víctima con dicha restitución. Probablemente éste sería un supuesto en el que el restablecimiento a la situación previa al ciberataque conllevaría la realización de un ingente número de tareas de muy difícil consecución. Si se piensa en todas las situaciones jurídicas que pudieran verse comprometidas por un ataque armado

378 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional. Internacional Humanitario Consuetudinario, op. cit.; pp.607-609.
379 *Ibidem*; pp. 616-617.

en las circunstancias que se han descrito, con toda probabilidad la indemnización y las medidas de aseguramiento de no repetición, serían más ventajosas para la entidad financiera, que la restitución, casi imposible en muchos aspectos.

Por último, el tema que nos ocupa obliga a realizar una reflexión en torno a la reparación que pudiera exigirse en relación a lo que la Compilación de DIH denomina "*grupos armados de oposición*", por cuanto la Norma 150 advierte de que "*Existe practica que indica que los grupos armados de oposición deben proporcionar una reparación apropiada por los daños resultantes de violaciones del derecho internacional humanitario*[380]."

En principio, se trata de una cuestión que conceptualmente pudiera parecer alejada de la que aquí se trata, pues el presente estudio se circunscribe a la responsabilidad internacional en que incurra el Estado. Sin embargo, habida cuenta las cuestiones de atribución del hecho ilícito que han sido tratadas en el Capítulo precedente, es preciso aquí realizar una somera mención al hecho de que la violación de una obligación internacional puede deberse al comportamiento de los agentes no estatales, en el sentido abordado en el citado Capítulo. En tal caso y, siempre que concurran las circunstancias allí expuestas, nacerá para el Estado al que se atribuya la conducta, la responsabilidad de reparar[381].

6.1.4 La prohibición de la perfidia.

Esta limitación impuesta por el DIH a los métodos de combate, pretende evitar el uso malicioso de bienes, dignos de una especial protección, al objeto de impedir, asimismo, un ataque militar que los utilice a modo de escudo.

La materialización de este principio se contiene en el artículo 37, del PA I, que establece la prohibición de matar, herir o capturar a un adversario, valiéndose de medios pérfidos. Se entiende, por lo tanto, la perfidia, como el

380 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Internacional Humanitario Consuetudinario, op. cit.; p. 620.
381 La Compilación de DIH cita, asimismo, la práctica de las "*Naciones Unidas que respalda la obligación de los grupos armados de oposición de ofrecer una reparación adecuada*". *Ibidem*; p. 621.

abuso de la buena fe de un adversario. Como consecuencia de ese abuso, se dará a entender al adversario que, quien esta actuando en el combate, tiene derecho a esa especial protección.

De entre las acciones que el referido Protocolo recoge como ejemplos de perfidia[382], no es difícil visualizar la posibilidad de que, algunas de ellas, cuando no todas, puedan cometerse por medios cibernéticos. A través de la red podrá simularse, por ejemplo, la intención de negociar bajo bandera de parlamento o de rendición o el estatuto de una persona civil. La realización de tales actividades no sólo contravendría lo dispuesto en el DIH convencional, ya citado, sino también el Consuetudinario, que prohíbe tal práctica, en la Norma 65 de la Compilación de DIH Consuetudinario. Dicha Norma, resulta de especial interés por cuanto y ofrece un listado de actividades pérfidas que resulta más detallado, que el contenido en el DIH convencional[383].

En cualquier caso, se exige que, entre el acto pérfido y la muerte, herida o captura del adversario, pueda constarse una relación causal. *A priori*, nada impide que esa causa esté constituida por un elemento cibernético, a través del que se simulara poseer estatuto civil o de protección y, con ello, indujera a error a quien recibiera dicho mensaje. Este error podría producirse, bien a través de la consulta de una página web o de un mensaje, comunicado a través de redes sociales, o de cualquier otro modo, utilizando la red. Si, de ese error, basado en el abuso de la buena fe del receptor, se derivaran las antedichas consecuencias, el acto resultaría ilícito, de igual modo que si ese mismo error hubiera sido causado por otros medios.

382 El artículo 37. 1 del PA I enumera como ejemplos de perfidia:" *a) simular la intención de negociar bajo bandera de parlamento o de rendición; b) simular una incapacitación por heridas o enfermedad; c) simular el estatuto de persona civil, no combatiente; y d) simular que se posee un estatuto de protección, mediante el uso de signos, emblemas o uniformes de las Naciones Unidas o de Estados neutrales o de otros Estados que no sean Partes en el conflicto*".

383 En el citado texto se enumeran las siguientes actividades: simular invalidez por heridas o enfermedad; simular una rendición; simular un intento de negociación bajo una bandera blanca; simular un estatuto de persona protegida utilizando el emblema de la cruz roja o de la media luna roja; simular un estatuto de persona protegida empleando los emblemas, las insignias o los uniformes de las Naciones Unidas; simular un estatuto de persona protegida utilizando otros emblemas protectores; simular el estatuto de persona civil; llevar los uniformes o utilizar los emblemas de Estados neutrales u otros Estados que no participen en el conflicto. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario Internacional Humanitario Consuetudinario, op. cit.; p. 250.

Esta prohibición, aplicada a los ataques informáticos, implica la ilicitud del ataque a redes, pertenecientes a entidades especialmente protegidas, cuando se realice con la finalidad de transmitir información de contenido militar[384]. En cualquier caso, resulta evidente que la acción pérfida puede ser realizada, a través de medios cibernéticos, aun cuando existen determinadas posturas que expresan lo contrario y que entienden que la vulneración de confianza constituye un elemento subjetivo y humano, que no puede producirse utilizando medios de naturaleza virtual[385]. Sin embargo, parece mas acertado defender la postura contraria y, en consecuencia, admitir que con el uso de estos medios, la ejecución de cualquier el engaño resulta más sencilla, por lo que todavía resulta más conveniente, tener presentes los elementos constitutivos de la perfidia.

En primer lugar, las actividades constitutivas de perfidia se definen, de forma negativa, de conformidad con lo dispuesto en el párrafo 2 del artículo 35 del PA I, que declara la licitud de las estratagemas como el camuflaje, las añagazas, las operaciones simuladas y las informaciones falsas. Por lo tanto, conviene tener presente el deslinde entre unas y otras actividades, sin que sea relevante, aquí, el medio a través del que se traiciona la confianza del combatiente que, finalmente, resulta engañado[386]. Precisamente, por el hecho de que el engaño se basa en el factor humano, ningún elemento que pueda afectar a éste, ha de ser ignorado. Incluso en aquéllos casos en que el engaño no se produzca, directamente, sobre personas, sino sobre sistemas informáticos, la prohibición sería aplicable.

En los intentos que, hasta ahora, se han realizado por deslindar los actos pérfidos de aquéllos otros, que resultan ser meras estratagemas de guerra,

384 HUGES, R. *A treaty for cyberspace*, op. cit.; pp.537.

385 Esta es la opinión minoritaria recogida en el Manual de Tallin. SCHMITT, M.N. (General Editor). Tallin Manual on the International, op. cit.; p. 182.

386 La utilización, por ejemplo, de uniforme militar de la otra Parte en conflicto, ha sido considerado como un engaño lícito y no como perfidia. Sí puede constarse en el juicio contra OTTO SKORZENY y otros, en los que el Tribunal absolvió a los acusados. En la sentencia relativa al mismo, puede leerse: "*The (…) accused involved in this trial were all officers in the 150th Panzer Brigade commanded by the accused Skorzeny. They were charged with participating in the improper use of American uniforms by entering into combat disguised therewith and treacherously firing upon and killing members of the armed forces of the United States*". Trial of Otto Skorzenya and others General Military Government Court of the U.S. Zone of Germany 18th August to 9th September, 1947.The United Nations War Crimes Commission, *Law Reports of Trials of War Criminals*, vol. IX, 1949.

permitidas por el DIH, pueden encontrarse supuestos que, bien podrían ser cometidos a través de medios cibernéticos, incluso con mayor facilidad que, con los medios de los que, hasta ahora, han dispuesto los Ejércitos. Entre estas actuaciones, SHAPP menciona aquéllas que, a su vez, son citadas en el *Army Field Manual The Law of Land Warfare* y, entre las que se encuentran, fingir la rendición propia, con la intención de procurarse una ventaja o la retransmisión de un falso armisticio al enemigo para, de ese modo, inducir a la rendición[387]. De forma evidente, este tipo de actuaciones pueden realizarse utilizando la red. En ambos supuestos podría darse la situación de que dicha actuación se produjera, a través de internet, utilizando, para ello, las redes sociales. Este tipo de comunicación permite dar a conocer el acontecimiento que se desee, con una gran inmediatez y, además, aporta la ventaja de que su difusión es masiva.

La necesaria distinción entre objetivos civiles y militares obliga, como se ha visto a la identificación de cada uno de ellos, de forma que, la ausencia de dicha identificación conllevará la pérdida del estatuto de civil. Sin embargo, esa ausencia no ha de ser confundida con la perfidia, salvo que, con la misma, se persigan los propósitos analizados más arriba. En el caso de los elementos cibernéticos, idéntica afirmación puede realizarse y, de esta manera, la no identificación, por ejemplo, de una página web o de una dirección IP, como civil no constituirá, de por sí, un acto de perfidia, salvo que dicha carencia de identificación persiga el abuso de la buena fe de quien reciba esa información y, de ello , se deriven las consecuencias antedichas[388].

Por último, resulta obligada una breve referencia a las cuestiones relativas a ciber espionaje que ya han quedado expresadas en el epígrafe correspondiente y, a las que nos remitimos, no sin recordar que la adquisición de información, por los beligerantes, forma parte, de modo evidente, del desarrollo de un conflicto.

387 Así puede leerse en, SCHAAP A.J. *Cyber warfare operations: Development and use under International Law*. Air Force Law Review, vol. 64. 2009; pp.121-174, en particular, p.152.
388 Esta argumentación es expuesta en la Norma 60 del Manual de Tallin. SCHMITT, M.N. (General Editor). Tallin Manual on the International, op. cit.; p. 183.

En esta tarea, la desinformación jugará un papel similar a la perfidia, en función de cómo sea aquélla difundida[389].

Así, la interpretación de los actos, que sean constitutivos de perfidia y no meras tretas de guerra, se circunscribirán, como recoge el articulo 37 del PA I, a "*los actos que, apelando a la buena fe de un adversario con intención de traicionarla, den a entender a éste que tiene derecho a protección, o que está obligado a concederla, de conformidad con las normas de derecho internacional aplicables en los conflictos armados*". Dichas actuaciones completan la anterior definición y, en consecuencia, califican el asesinato, herida o captura del adversario como pérfidos. Además, la definición exige que, el comportamiento anterior traicione la buena fe del adversario y que, esa buena fe esté, directamente, relacionada con su creencia de tener «*derecho a protección (...) de conformidad con las normas de derecho internacional aplicables en los conflictos armados*».

Es decir, que no puede entenderse como acto pérfido aquél que no obtenga el resultado, recogido en el artículo citado, ni aquél que traicione la buena fe del adversario, que se fundamente en cualquier otro motivo, distinto de la protección especial que otorga el DIH[390]. El mismo artículo 37 del PA I ofrece los siguientes ejemplos de perfidia:

> "(a) simular la intención de negociar bajo bandera de parlamento o de rendición;
> (b) simular una incapacitación por heridas o enfermedad;
> (c) simular el estatuto de persona civil, no combatiente; y
> (d) simular que se posee un estatuto de protección, mediante el uso de signos, emblemas o uniformes de las Naciones Unidas o de Estados neutrales o de otros Estados que no sean partes en el conflicto".

A la vista de los ejemplos anteriores, no parece extraño apreciar la comisión de perfidia, por medios cibernéticos. Antes bien, las posibilidades ofrecidas por internet, antes mencionadas, así como todas aquéllas que, obtenidas

389 Así lo explica SCHAAP: «*Because cyber espionage is likely to become an important intelligence gathering tool, states will likely plant misinformation on their own networks to confuse or mislead the enemy. Such misinformation is synonymous with any other method for delivering misinformation*». SCHAAP, A.J. *Cyber warfare operations: Development and use under International Law*, op. cit.; p.152.
390 Esta conclusion es alcanzada, asimismo, por KALSHOVEN, F. y ZEGVELD, L. Restricciones en la conducción de la guerra. Introducción al derecho internacional humanitario. Comité Internacional de la Cruz Roja. Ginebra, marzo de 2001; pp. 108-110.

por en el uso de las nuevas tecnologías, pudieran difundirse por la red, favorecerían la realización de este tipo de actos.

La simulación de la intención de negociar o, del estatuto de no combatiente, del estatuto de protección y, aun, de la incapacitación por heridas o enfermedad, bien podrían trasladarse al enemigo por medios informáticos, a través de correos electrónicos falseados, mensajes en las redes sociales o, la difusión de vídeos que originaran confusión. En estos supuestos, de sencilla realización por cualquier parte combatiente, será imprescindible la distinción anteriormente apuntada y, por lo tanto, apreciar la concurrencia de los dos elementos apuntados para la apreciación de perfidia y, en consecuencia, de la violación de una norma de DIH. No es ocioso señalar que, precisamente, la facilidad en la realización de este tipo de actividades, así como el alcance generalizado de los medios informáticos, podrían originar que tales conductas se cometieran, sin la intención o resultado, anteriormente apuntados, incluso por quien, simulando ser combatiente, no gozara de dicho estatuto.

El surgimiento de la responsabilidad internacional como consecuencia de la violación de esta obligación implicara, como en los casos ya vistos, que el Estado lesionado exija la cesación en la violación y el consiguiente cumplimiento de la obligación. Asimismo, resultara viable la exigencia de cualquiera de las medidas de reparación que, posteriormente se verán con más detalle. No obstante, considerando el contendido de la obligación hasta ahora examinada, no parece que determinadas medidas previstas en el proyecto resulten aquí viables. Ya se ha expuesto, cómo la comisión de un hecho ilícito, a través de la pérfida, exige la producción de una serie de resultados, cuya restitución material resultara de imposible consecución. Por lo tanto, en este supuesto serán de aplicación las consecuencias que, posteriormente, van a ser objeto de atención.

6.1.5 El respeto a la neutralidad de terceros.

La neutralidad es la condición del Estado, que no es Parte Beligerante en un conflicto armado internacional, de forma que el estatuto de neutralidad no

dependerá de la declaración de la misma, ni de la posición que tomen los Estados al respecto.[391]

Esta norma está considerada una norma de DIH Consuetudinario[392], de forma que las dudas que pudieran existir motivadas por su posible obsolescencia[393], han de quedar despejadas a favor de su completa vigencia.

El principio de neutralidad se establece con el objetivo de respetar a aquellos Estados que, en caso de conflicto, no deseen aliarse, con los Estados combatientes. No sólo impone obligaciones a los Estados que, así se han declarado, sino también a los que libran la contienda, respecto de aquéllos. Si tenemos en cuenta que internet puede considerarse un arma de guerra, habrá que atender a la posibilidad de que pueda producirse una declaración de neutralidad y, atender, en consecuencia, las situaciones en que la misma ha de respetarse. Este respeto de la nautralidad debera observarse, inclsuo, cuando la misma no haya sido declarada expresamente. El principal problema, al respecto, vendrá dado por la dificultad de determinar las fronteras del Estado, que se declara neutral, toda vez que internet constituye una red virtual y global. En consecuencia, el criterio de la territorialidad, necesitará de una reinterpretación que permita su aplicación a este contexto. Para ello, será necesario acudir a criterios tales como, la ubicación de la IP utilizada para lanzar el ataque o al lugar físico en el que se produzcan los efectos del mismo.

La obligación del respeto a la neutralidad impedirá, en primer lugar, que los beligerantes utilicen el territorio de un Estado neutral, para el movimiento de sus tropas o, de su material. Nuevamente, las aportaciones que introduce este elemento cibernético en el desarrollo de los conflictos armados plantean la necesidad de abordar situaciones que, hasta ahora, no habían sido objeto de estudio. Así, hay que tener presente la posibilidad de que, los ataques se produzcan a través de, lo que se ha venido a llamar, equipos zombie, es decir,

391 En este sentido se pronuncia la Norma 167 de la obra AA.VV. Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare. Program on Humanitarian Policy and Conflict Research at Harvard University. Berna. Mayo 2009; pp. 308-309.
392 Legality of the Threat or Use of Nuclear Weapons, doc. cit.; par. 89.
393 En tal sentido se expresa VON HEINEGG, W. H. *Territorial Sovereignty and Neutrality in Cyberspace*. International Law Studies. U.S. Naval War College, vol. 89, 2013; pp. 123-156.

aquéllos físicamente emplazados en un lugar distinto del que utilizan para operar, ocultando su verdadero origen[394].

En este caso, nuevamente, se constatarán dificultades de índole técnico, a la hora de determinar el lugar de origen del ciberataque, así como el Estado o, la persona a quien atribuirlo. Sin embargo, como se viene repitiendo, esos obstáculos de carácter práctico, no pueden conllevar un aminoramiento en el cumplimiento del DIH. En efecto, puede ocurrir que dichas identificaciones resulten complejas, incluso que el Estado cuyas redes están siendo utilizadas para lanzar el ciberataque, desconozca tal circunstancia, pero en ningún caso, puede renunciarse a la protección de dicha neutralidad, derivada del ejercicio de la soberanía del Estado en cuestión[395].

En virtud de esta obligación, por lo tanto, deberá protegerse la infraestructura cibernética localizada en territorio neutral. Los Estados neutrales no podrán implicarse en ciberactividades, de apoyo a las acciones militares de uno de los beligerantes, en detrimento de la otra parte del conflicto. Además, estarán obligados a tomar las medidas apropiadas para poner fin al uso malicioso, por parte de los beligerantes, de la infraestructura cibernética situada en su territorio[396]. En definitiva, los beligerantes se abstendrán de hacer ejercicio de sus derechos utilizando para ello la ciberinfraestructura situada en territorio neutral.

El respeto a la neutralidad cobra una especial relevancia, en el caso de los ataques, utilizados como medio de combate porque, aunque los ciberataques pueden ser programados con precisión, su transmisión geográfica no puede ser, completamente controlada, de forma que, siempre se pueda evitar el uso de infraestructura de comunicaciones neutral[397]. Toda vez que el DIH convencional, aplicable en este caso, prevé una excepción, relativa al uso de las comunicaciones de Estados neutrales, resulta determinante esclarecer si, las transmisiones realizadas a través de dicha infraestructura, lo son de sistemas de guerra o, de

394 En este sentido, puede verse HATHAWAY, O. A. y otros. *The law of cyber-attack*, op. cit.; p. 860.
395 También se pronuncia en este sentido el grupo de expertos. SCHMITT, M.N. (General Editor).Tallin Manual on the International, op. cit.; pp. 248-256.
396 VON HEINEGG, W.H., *Territorial Sovereignty and Neutrality in Cyberspace*, op. cit. pp. 123-156.
397 MELZER, N., *Cyberwarfare and International Law*. UNIDIR resources. 2011; p.20. Documento disponible en el sitio web: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. Fecha de consulta, junio 2014.

meros datos de comunicación. Así, al respecto, el artículo 8 del V Convenio de La Haya, Relativo a los derechos y a los deberes de las Potencias y de las personas neutrales, en caso de guerra terrestre de 1907, ya establecia que, "*Una Potencia Neutral no está llamada a prohibir el uso de parte de los beligerantes del telégrafo o de los cables telefónicos o de aparatos inalámbricos de telegrafía que pertenezcan a él, a compañías o a particulares*".

Sin embargo, como se viene manteniendo, internet es, naturalmente, un medio de comunicación y transmisión de la información, pero su uso no queda limitado a ello, sino que sus posibilidades son netamente mayores. Por ello, la interpretación de determinados conceptos no puede quedar constreñida a la concepción que, de dichos medios de comunicación, se haya realizado tradicionalmente. La complejidad e interdependencia de las actuales redes de comunicación ha llevado, a algún autor, a entender que, ese control efectivo y eficaz, que impida el uso de las comunicaciones, no resulta posible con internet[398]. Tal como pone de relieve VON HEINEGG, la práctica de los Estados, especialmente la observada en las ciberoperaciones que se desarrollaron durante la campaña de Kosovo o, en el conflicto ya mencionado de Georgia, demuestran que una ciberoperación, que tenga por objeto, incluso la transmisión de armas cibernéticas y se desarrolle a través de una ciberinfraestructura neutral, no viola la neutralidad de los Estados a través del que pasan dichas transmisiones.

En el caso de los DDoS[399] lanzados contra Georgia, no pudieron asimilarse a la transmisión de "*munición de guerra*" y por lo tanto, no tuvieron la consideración de ataques armados, motivo por el cual, se concluyó que no violaban la obligación de neutralidad[400]. Esta práctica, por otra parte, también responde a la construcción doctrinal que, al respecto, se ha realizado en cuanto a la obligación de respeto a la neutralidad en el uso de ciberinfraestructuras[401].

---

398 Así lo recoge VON HEINEGG W.H., *Territorial Sovereignty,* op. cit.; p. 149

399 La definición de DDoS que ofrece el Manual de Tallin es la siguiente: "*Distributed Denial of Service (DDoS): A technique that employs two or more computers, such as the bots of a botnet, to achieve a denial of service from a single or multiple targets*". SCHMITT, M.N. (General Editor). Tallin Manual on the International Law, op. cit.; p. 259.

400 VON HEINEGG, W.H., *Territorial Sovereignty*, op.cit.; p. 149.

401 Esta conclusion viene, asimismo, amparada por la obra, Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare, cuya Norma 168 b), establece:

En cualquier caso, en la materia que ahora nos ocupa será imprescindible acudir a la práctica de los Estados, por cuanto, será de este modo cómo se interpretarán los conceptos que, por el momento, todavía quedan difusos, sin olvidar la influencia positiva que dicha constatación puede tener en la voluntad de los Estados de alcanzar el consenso en normas que moderen la ciberactividad[402].

Por otra parte, no sólo los beligerantes han de respetar el principio que aquí se expone. También los terceros Estados contraen obligaciones respecto de los neutrales. Estas obligaciones se circunscriben a la prohibición de permitir o, tolerar el ejercicio de los derechos de beligerantes, en su territorio; de poner fin y prevenir la violación de su neutralidad por un beligerante y de aceptar la imposición de la neutralidad por el beligerante agraviado, tal y como puede leerse en el aludido artículo 5 del V Convenio de La Haya. El referido Convenio establecia, a su vez, que una Potencia neutral no puede permitir que ninguno de los actos referenciados en los artículos 2 a 4 tenga lugar en su territorio. En el presente caso, pues, no podrá permitir el ejercicio de los derechos de los beligerantes, usando la ciberinfraestructura ubicada en su territorio o de aquélla que, estando ubicada fuera de él, esté sometida a su absoluto control.

Esta obligación de poner fin y prevenir la violación de su neutralidad por parte de un beligerante, en todo caso, implica la valoración de los medios de que disponga el Estado neutral. Si esto resulta obligado en todo caso porque se obliga a la adopción de todas las medidas razonables para ello, en el caso de internet, todavía habrá que tenerlo más presente, habida cuenta el desequilibrio de medios entre distintos Estados, lo que, de modo evidente, conllevará una mayor colaboración entre los Estados, a fin de alcanzar el objetivo expuesto.[403] En

---

"*…when Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality.*"; op. cit.; p. 310-312.

402 Así se expresan BROWN, G. y POELLET K., *The Customary International Law of Cyberspace.* Strategic Studies Quarterly. Fall 2012; pp. 126-145, en particular, p. 141.

403 De este modo lo entiende VON HEINEGG, cuando afirma que: "*…governments should cooperate with a view to improving their capabilities in the area of cyber forensics. Such cooperative efforts are necessary not only in order to identify attackers, but also to establish a more effective deterrent of malevolent States and non-State actors.*", VON HEINEGG, W.H., *Territorial Sovereignty,* op. cit.; p.156.

cualquier caso, los beligerantes a quienes se les impida el ejercicio de sus ciberactividades en territorio neutral, no pueden considerar que se esté cometiendo un acto hostil, sino que habrán de soportar las medidas de cese que se impongan.

El incumplimiento, por parte de un Estado, de las antedichas obligaciones, podrá justificar la respuesta por la fuerza del Estado lesionado. El beligerante perjudicado por la inobservancia de la neutralidad, está legitimado para su adopción, en aquéllos supuestos en que, el Estado neutral no haya sido capaz o, no haya manifestado su voluntad, de cumplir con su obligación de evitar la infracción[404]. Sin embargo, no toda violación de neutralidad por uno de los beligerantes justificará la respuesta por el otro. Antes bien, dicha respuesta quedará limitada a los supuestos en que dicha violación tenga un impacto negativo en la seguridad de los intereses del beligerante, pero no, por ejemplo, cuando la ciberinfraestructura de un Estado neutral no aporta ventaja militar al otro beligerante. En este caso la respuesta quedará reservada al Estado neutral. El beligerante agraviado, pues únicamente podrá responder a la amenaza si la violación de la neutralidad constituye una amenaza grave e inmediata para su seguridad, no hay alternativa factible y la medida adoptada es necesaria y proporcionada a la amenaza causada por la violación.

Nuevamente, la situación vivida por el estado de Georgia, revela hasta qué punto la cuestión de la neutralidad puede resultar relevante, porque en los supuestos en que la ciberinfraestructura quede gravemente dañada y no pueda utilizarse por el Estado en conflicto o, cuando su empleo constituya un riesgo para el Estado combatiente, este podrá plantearse el uso de la ciberinfraestructura

404 Así puede leerse en Manual de San Remo sobre el Derecho Internacional aplicable a los conflictos armados en el mar que, al respecto establece que: "*Si el Estado neutral no pone término a la violación de sus aguas neutrales por un beligerante, el beligerante adverso deberá notificarlo al Estado neutral y concederle un tiempo razonable para que acabe con dicha violación. Si la violación de la neutralidad de un Estado por parte de un beligerante constituyera una amenaza grave e inmediata para la seguridad del beligerante adverso y no hubiera cesado, este Estado beligerante, a falta de otra alternativa factible y oportuna, podrá usar la fuerza estrictamente necesaria para responder a la amenaza que constituye la violación*". AA.VV. (ed. Louise Doswald-Beck). San Remo Manual on International Law Applicable to Armed Conflicts at Sea. Prepared by a Group of International Lawyers and Naval Experts convened by the International Institute of Humanitarian Law, 1995. Parte II, Sección 1; par.22.

radicada en un otro Estado. Asi ocurrio en este caso cuando Georgia, en palabras de KASTENBERG "*took an unorthodox step and sought "cyber refuge" in the United States*"[405], cuando su Gobierno quedó bloqueado, desde el punto de vista de sus comunicaciones por internet, a resultas de los ataques sufridos.

Una vez acreditada la violación de la obligación, surge de nuevo la cuestión del contenido que la relación jurídica de responsabilidad internacional deberá presentar, como mas adecuado para satisfacer la reparación. En primer lugar, hay que plantearse si la obligada cesación del hecho ilícito es viable o no. Si se trata, por ejemplo de un ataque que ha introducido un virus informático, en un sistema militar, violando el deber de respetar la neutralidad, porque se dirige a un Estado que se ha declarado, así, en el conflicto, habrá que examinar si realmente el virus se puede detener. En el citado supuesto del virus Stuxnet, la producción de sus efectos difícilmente se hubiera podido producir de forma automática, una vez introducido el virus, en el sistema informático de la central nuclear. Por lo tanto, el hecho ilícito podrá detenerse, en la medida en que ello sea técnicamente posible.

Por otra parte, la cesación del hecho ilícito implica la valoración, de todas las acciones u omisiones que lo componen[406], de modo que, si el ilícito se estuviera produciendo, como consecuencia de una omisión, esta nueva responsabilidad podrá consistir en una conducta activa como, por ejemplo, impedir que grupos organizados usen la red de un Estado, para participar en las hostilidades contra otro. El Estado que está recibiendo los ataques armados, a través de internet, podrá entender que el Estado infractor no realiza ninguna acción para impedirlo y que, por lo tanto, está violando una norma de DIH, por ejemplo, la de respetar la neutralidad de un tercero, aquí vista. En ese caso, el

405 El autor relata el apoyo recibido por parte de los Estados Unidos de la siguiente manera: "*Without first seeking U.S. government approval, Georgia relocated its Presidential website to a U.S. web hosting company and moved its Ministry of Foreign Affairs (MFA) press dispatches to Google's Blogspot. The MFA also mirrored its Internet services at a site in Estonia and on the website of Poland's president, Lech Kaczynski*". KASTENBERG, J.E., *Non-intervention and neutrality in cyberspace: an emerging principle in the national practice of International Law.* Air Force Law Review. Cyberlaw edition, vol. 64, 2009; pp.43-64, en particular, p. 47.

406 Ello es así, "*con independencia de si el comportamiento del Estado es una acción u omisión ... ya que puede haber una cesación consistente en abstenerse de determinadas acciones (...)*". Comentario 2) al artículo 30 del Proyecto.

Estado lesionado podría requerir una actuación del primero, que impida la continuación del ciberataque.

Igualmente, cuando la violación de la obligación internacional, presente el contenido visto en este apartado, parece coherente, con ese respeto a la neutralidad que ha sido violado, que el Estado perjudicado, exija la adopción de seguridades y garantías adecuadas de no repetición. En el ámbito que aquí se estudia, esto implicara la adopción de una serie de compromisos, más que de medidas reales. En el caso de que en el desarrollo del combate se incumpla una norma de DIH conllevará el surgimiento de la obligación de cesar en la infracción y de reparar, si a ello hubiera lugar. Sin embargo, si el Estado perjudicado exigiera la adopción de garantías de no repetición, cabría adoptarlas bajo compromiso del infractor y otorgando medidas protectoras desde un punto de vista material, al Estado perjudicado, a cuenta del infractor.

El Comentario al Proyecto, en su artículo 30, advierte de la posibilidad de que las seguridades y garantías de no repetición sean requeridas por un Estado distinto del lesionado. En ese caso, podría darse el supuesto de que Estados que son socios comerciales, exigieran del infractor, que no se volviera a repetir el ataque a una entidad bancaria con la que, empresas nacionales suyas, tuvieran negocios en marcha. No puede decirse que el Estado C sea lesionado, pues el conflicto bélico se dirime entre A y B. Sin embargo, el hecho de infringir la norma de DIH contra B, puede perjudicar los intereses económicos de C y exigir éste el tipo de garantías y seguridades que prevé el Proyecto. En este caso, el compromiso del Estado de no volver a repetir la infracción de esa o cualquier otra norma de DIH, podría venir acompañado de medidas técnicas, tales como el robustecimiento de medidas de seguridad para el sistema financiero, adoptadas o sufragadas por el Estado A, infractor. No puede olvidarse en ningún caso la tan repetida salvaguarda, realizada por el Comentario al Proyecto, en relación con la naturaleza de la obligación. En efecto, en determinados casos resultará inviable la adopción de un compromiso de no repetición.

En el caso que aquí se prevé, no resulta imposible. La violación de las obligaciones de DIH tanto por acción como por omisión, implicara, en gran

medida, la realización de un acto voluntario o la omisión grave de la diligencia debida. Por tal motivo, el compromiso de no repetición pudiera en estos supuestos hallar una relevancia suficiente.

Además de la cesación en la infracción y el cumplimiento de la obligación que hasta ese momento estaba siendo violada, la responsabilidad exige, en su momento más inicial, que se proceda a la reparación del perjuicio.

No obstante, la existencia de un daño económico no parece ser requisito imprescindible para el surgimiento de la responsabilidad internacional del Estado. Es decir, como ya se ha adelantado, la responsabilidad internacional constituye una relación jurídica nueva, distinta de la que ha sido violada y nace, precisamente de dicha infracción. Y ello resulta a sí con independencia de la existencia o no de un daño económico. La existencia de tal daño será determinante únicamente, a la hora de hallar el modo más efectivo de reparar el perjuicio sufrido.

La reparación es, por lo tanto, una consecuencia y no un derecho del Estado y, por ese motivo resulta irrelevante si se exige o no y quien lo hace[407]. En definitiva, resulta determinante la acreditación de la violación de la obligación, de forma que el objeto de la reparación es, en términos generales, el perjuicio causado por un hecho ilícito y no todas y cada una de las consecuencias dimanadas de un ilícito[408]. Ello implica que el daño sigue siendo irrelevante a la hora de determinar la existencia de la reparación, aunque no la forma en que se lleve a cabo. En el ataque informático a la entidad bancaria, podría exigirse una reparación acorde con las consecuencias, pero es la violación de la norma de DIH que obliga a distinguir objetivos civiles y militares la que determina la existencia de la obligación de reparar[409].

Por último y, con carácter general, aplicable, por lo tanto, a la mayoría de los supuestos aquí tratados, el Proyecto, establece la posibilidad de exigir

407 Comentario 4) al artículo 31 del Proyecto.
408 Comentario 9) al artículo 31del Proyecto.
409 También puede leerse tal afirmación en la Norma 149 de la Compilación de DIH Consuetudinario. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; pp.599-606.

indemnización, cuando la restitución no haya sido posible[410]. En palabras de PÉREZ GONZÁLEZ, la indemnización tiende a "*cubrir cuantitativamente además de lo debido por equivalencia, el resarcimiento de los daños sufridos que no hayan sido reparados por...el pago efectivo*[411]". De forma prácticamente idéntica se recoge dicho mecanismo en el artículo 36 del Proyecto. Ya se ha anticipado cómo, por ejemplo, los daños causados a través de la perfidia serán de difícil cuando no imposible restitucion material. En este caso y, en otros de similar naturaleza, cobra importancia la prevsion del Proyecto, que ahora s expone.

En los supuestos de violación de las obligaciones de DIH, aquí estudiadas, podrá ocurrir que el restablecimiento de la situación al momento previo al ataque armado, que se ha producido a través de internet, sea de muy difícil precisión, pues el propio conflicto añadirá incertidumbre a la situación. Por este motivo la indemnización se trata de una medida reparadora de gran interés para el supuesto de la violación de normas de DIH.

De este modo, el PA I estipula que todo Estado que viole el DIH deberá hacer efectiva una indemnización cuando proceda[412]. No obstante, en los supuestos que aquí se han ido exponiendo, este modo de reparación encontrará una dificultad adicional, a la hora de hacerse efectivo, que es la necesidad de la acreditación de un daño real. Ya se ha tratado, la irrelevancia de la existencia del daño en la acreditación de la responsabilidad internacional, en paralelo con su importancia en la elección del medio de reparación. Será aquí, pues, donde el daño efectivo haya de ser constatado, de forma tal que no podrá darse indemnización de otro modo que no sea respecto del "*daño susceptible de evaluación financiera, sufrido por el Estado lesionado o sus nacionales*." Así, la indemnización se presenta como un mecanismo de reparación, coherente, por

410 El Proyecto reconoce el carácter subsidiario de la indemnización, en su artículo 36, cuando entiende que "*El Estado responsable de un hecho internacionalmente ilícito está obligado a indemnizar el daño causado por ese hecho en la medida en que dicho daño no sea reparado por la restitución*".

411 PEREZ GONZALEZ, M., *La responsabilidad internacional (I): el hecho internacionalmente ilícito,* op. cit.; p. 879.

412 De este modo se recoge en la Norma 150 de la Compliacion de DIH Consuetudinario que, a su vez remite al contenido del artículo 91 del PA I. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; p. 609.

ejemplo, con la responsabilidad surgida de la violación de la obligación internacional de que prohíbe la causación de daños desproporcionados.

En el caso del ciberataque a las infraestructuras críticas que se ha expuesto, la acreditación de ese daño será efectiva, aunque de difícil cuantificación, pues como también se ha adelantado, la diversidad de consecuencias de la violación de la norma de DIH dificultará la concreta prueba de cada uno de los perjuicios. En cualquier caso, la extensa dimensión que pueda llegar a alcanzar tal medida no puede en modo alguno permitir que ello devenga en un castigo al Estado infractor, ni que se adopte a título ejemplarizante[413]. En cualquier caso, no cabría duda de la obligación de indemnizar en un supuesto como el planteado en el que el objeto del ataque lo constituye una entidad bancaria, incluida, como se ha expresado en el catálogo de Infraestructuras Críticas. La obligación se extiende a minorar los daños sufridos por el Estado y sus nacionales "*sean personas físicas o jurídicas, en cuyo nombre el Estado presenta una reclamación en el marco de la protección diplomática*[414]".

Si bien ya se ha apuntado el carácter subsidiario de la indemnización, en relación con la restitución, es preciso aquí poner en evidencia el protagonismo de este modo de reparación en el caso de las violaciones de DIH a través de ciberataques. Esto será así, previsiblemente, por cuanto la restitución a la situación inicial será prácticamente imposible en buena parte de los casos. En el caso de la violación de la obligación de DIH que obliga a distinguir entre objetivos civiles y militares, la indemnización abarcaría la reparación de todos los daños económicos producidos. Estos daños, asimismo, abarcan los causados al Estado al que pertenezca el bien atacado o, en el que radique y, también, a la propia empresa, pues ha de entenderse que, si se admite la indemnización a empresas nacionalizadas[415], con igual motivo habrá que admitirlo respeto de empresas que, por ejemplo, formen parte de la red de infraestructuras críticas, conforme a los criterios que se expondran en otra parte del presente trabajo.

413 Comentario 4) al articulo 36 del Proyecto.
414 Comentario 5) al articulo 36 del Proyecto.
415 Comentario 23) al articulo 36 del Proyecto.

Si a través de la violación de la aludida obligación internacional, un hospital, sufriera un ciberataque, no cabe duda de que surgiría la correspondiente responsabilidad internacional para el Estado infractor. Dicha responsabilidad debería exigirse por más que dicho hospital no fuera gestionado por el Estado, sino por una entidad privada. La pertenencia de una empresa privada a la red de infraestructuras críticas del Estado, como se vera con mayor profundidad en el epígrafe correspondiente, impone a sus responsables una serie de obligaciones, en materia de ciberseguridad, pues las mismas se encuentran en una posición de vulnerabilidad mayor que el resto. Por este motivo y por la importancia de las funciones que estas desempeñan, ha de abogarse por la obligación de restablecer a estas empresas al estado en que se hallaren con anterioridad al ciberataque.

Ciertamente, ni una tarea ni otra resultará sencilla por el hecho, también apuntado anteriormente, de que la evaluación económica de los daños causados [416] exigirá un análisis equivalente a poner en evidencia las vulnerabilidades del sistema de seguridad informática. Dicha tarea no sólo puede resultar compleja desde un punto de vista técnico sino, sobre todo desaconsejable, por cuanto implicaría asumir futuros ataques y supondría, por ende, una pérdida de valor económico de dicha empresa.

En consecuencia, parece que ambas formas de reparación pueden presentar inconvenientes de tipo práctico en el caso de violaciones de DIH a través de ciberataques, de manera que, en la aplicación subsidiaria de los modos de satisfacer la responsabilidad del Estado, será necesario atender a la satisfacción como última de las modalidades previstas.

El carácter amplio con el que esta medida reparadora se contempla en el Proyecto se refleja, asimismo, en el párrafo segundo del artículo 36, que prevé que la indemnización comprenda también "*el lucro cesante en la medida en que éste sea comprobado*." Surgirán aquí dificultades de prueba ligadas a la necesidad de

416 Dicha evaluación económica queda expresamente exigida en el Comentario 4) al artículo 36.

acreditación efectiva, toda vez que se desestima la indemnización de daños demasiado remotos o indirectos[417].

Para terminar, cuando la restitución material y/o jurídica de la situación previa al ataque resulta inviable y, la indemnización de los daños económicos tampoco es posible, el Proyecto de artículos ofrece, como última posibilidad, la figura de la satisfacción y, así su artículo 37, faculta a poner en marcha este mecanismo, "*en la medida en que ese perjuicio no pueda ser reparado mediante restitución o indemnización*".

La figura de la satisfacción resultará especialmente oportuna en aquellos casos en los que no se haya producido un daño económico confirmando, así, como en numerosas ocasiones se ha afirmado, que la producción de dicho daño económico no es imprescindible para hacer surgir la relación jurídica de la responsabilidad internacional. Asimismo, supondrá también una medida adecuada en los casos en que los perjuicios constatados no permitan una evaluación económica.[418] Se tratará de supuestos en los que, por ejemplo, se haya violado el deber de neutralidad o se haya cometido un ciberataque sin necesidad militar. En ambos casos, la producción del daño material, evaluable económicamente, no es consustancial la violación. En el caso, por ejemplo, de los ciberataques sufridos por Georgia, durante el conflicto bélico y, que ya han sido expuestos, el daño económico, si lo hubo, es irrelevante. Para un Estado en combate, parece más determinante mantener sus comunicaciones que evitar el daño económico que su restauración pudiera acarrear. Por lo tanto, en supuestos similares, las medidas de satisfacción al Estado lesionado que se van a exponer, supondrán la última posibilidad de ver reparada la violación de la obligación internacional.

Dentro del concepto de satisfacción pueden encontrarse diversas manifestaciones y ha de entenderse comprendida cualquiera que dé

417 Comentario 10) al artículo 31 del Proyecto.

418 A juicio de PEREZ GONZALEZ, la satisfacción es una "*forma particularmente adecuada para enjugar los daños "morales" ocasionados al Estado (ofensa al honor o la dignidad), aunque puede concurrir con otras formas de compensación en relación con violaciones de diversa especie, pues, como se ha dicho, aun en caso de no mediar ataque expreso a la dignidad del Estado la simple tolerancia de una violación de DI, es adecuada para disminuir el prestigio del Estado ofendido*". PEREZ GONZALEZ, M., *La responsabilidad internacional (I): el hecho internacionalmente ilícito*, op. cit.; p. 877.

cumplimiento al deber de reparar. Es decir, como satisfacción podrá entenderse cualquier actitud que el Estado infractor adopte respecto del perjudicado y así, el Proyecto cita textualmente "*un reconocimiento de la violación, una expresión de pesar, una disculpa formal o cualquier otra modalidad adecuada*[419]". Es evidente que cualquiera de estas modalidades resultaría aconsejable en el caso de una infracción de DIH que no conllevara la causación de un perjuicio económico. También ha de reputarse satisfacción la presentación de excusas, el castigo a los culpables, el pago de una suma simbólica, la verificación por una instancia imparcial internacional del carácter ilícito del hecho[420].

De entre todas las modalidades de satisfacción, parece que en el ámbito que aquí se trata, pudiera tener una especial relevancia el castigo a los culpables, por cuanto el DIH prevé específicamente la obligación de los Estados de investigar los crímenes de guerra para los que tengan jurisdicción y encausar a los sospechosos si procede[421]. En el ordenamiento jurídico español, esta obligación encuentra su primer fundamento en el Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas, por cuanto su Capítulo VI "*De la ética de las operaciones*", recoge la obligación del militar de conocer, difundir y aplicar, en el transcurso de cualquier conflicto armado u operación militar, las normas convencionales de DIH[422].

Como ya se puso de manifiesto junto con DE TOMÁS MORALES, con independencia de la falta de referencia a las normas consuetudinarias de DIH, el artículo 106 permite deducir que, en cualquier conflicto armado, incluida la ciberguerra, así como en cualquier operación militar, incluidas las

419 Párrafo 2 del artículo 37 del Proyecto de artículos.
420 Así aparecen citadas en los Comentarios 5) y 7) al artículo 37.
421 Así se recoge en la norma 158 de la Compilación de DIH Consuetudinario. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; pp. 687-690.
422 En concreto, las Reales Ordenanzas hacen mención expresa a "*los convenios internacionales ratificados por España relativos al alivio de la suerte de heridos, enfermos o náufragos de las fuerzas armadas, al trato a los prisioneros y a la protección de las personas civiles, así como los relativos a la protección de bienes culturales y a la prohibición o restricciones al empleo de ciertas armas*". Artículo 106, "Deberes en relación con el Derecho Internacional Humanitario". Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas, BOE núm. 33, de 7 de febrero de 2009.

ciberoperaciones, deben aplicarse las normas oportunas del DIH[423]. Además, la obligación de difundir las normas pertinentes de DIH, se encuentra recogida en el artículo 83 del Protocolo Adicional I[424].

Por lo que respecta a la necesidad de previsión, en la legislación interna, de "*sanciones penales efectivas para quienes cometan, u ordenen cometer cualquiera de estos graves incumplimientos*", en el caso español, serían de aplicación los delitos contenidos en el Título XXIV del Libro II del Código Penal, bajo la rúbrica "Delitos contra la Comunidad Internacional" (artículos 605 a 616 *quater*), sin que, en principio, la adopción de nuevos métodos de combate justifique una nueva interpretación[425].

La adopción pues, de medidas disciplinarias y penales, posteriores a la violación de una norma de DIH, podría interpretarse como una obligación independiente, cuyo cumplimiento no precisa de la exigencia de responsabilidad internacional del Estado. Sin embargo, siendo esto así, tampoco puede obviarse la función que esta medida puede cumplir como medio de satisfacción al Estado agraviado. En efecto, la adopción de medidas tendentes a satisfacer al Estado lesionado a través del castigo a los culpables, será una reparación adecuada en aquellos casos en que todos los mecanismos anteriores se hayan demostrado infructuosos.

---

423 DE TOMÁS MORALES, S. y VELAZQUEZ ORTIZ, A.P., *La responsabilidad del mando en la conducción de operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz*, op. cit; p. 129.

424 El citado artículo establece que "*1. Las Altas Partes contratantes se comprometen a difundir lo más ampliamente posible, tanto en tiempo de paz como en tiempo de conflicto armado, los Convenios y el presente Protocolo en sus países respectivos y, especialmente, a incorporar su estudio en los programas de instrucción militar y a fomentar su estudio por parte de la población civil, de forma que esos instrumentos puedan ser conocidos por las fuerzas armadas y la población civil.2. Las autoridades militares o civiles que, en tiempo de conflicto armado, asuman responsabilidades en cuanto a la aplicación de los Convenios y del presente Protocolo deberán estar plenamente al corriente de su texto*".

425 En los apartados 1 y 4 del artículo 615 *bis* de nuestro Código Penal se atribuye expresamente a autoridades y jefes militares; a quienes actúan *de facto* como tales y a superiores no incluidos en las anteriores categorías, una posición garante, resultado de considerar "*estructuralmente equivalentes la omisión y la causación activa del resultado en el supuesto de que no adopten las medidas a su alcance para evitar la comisión de los delitos mencionados por las fuerzas sometidas a su mando o control efectivo o por sus subordinados, respectivamente*", tal y como lo expresa con gran claridad Patricia Faraldo, quien añadirá que "*no es necesario acudir al artículo 11 CP, que regula la comisión por omisión, pues el legislador ya ha equiparado la omisión a la acción en este supuesto*". Véase FARALDO CABANA, P., *La responsabilidad por mando en el Código Penal español*, en Olásolo Alonso, H., y Cuenca Curbelo, S., (Coords.), *Perspectiva iberoamericana sobre la justicia penal internacional,* vol.I, 2011, Valencia, 2012; pp.171-185; en particular, p. 180.

Al analizar el contenido de la obligación de evitar la perfidia, se hacía mención al resultado de la violación de dicha norma, cuando entraña la comisión de un daño personal[426]. Pues bien, cuando la responsabilidad internacional surja de la violación de esta norma de DIH y se produzca la muerte de una persona, la restitución será ontológicamente imposible y la indemnización en determinadas situaciones será insuficiente. En consecuencia, el castigo al culpable, el reconocimiento de la infracción y el ofrecimiento de disculpas serán medidas viables y necesarias.

Además, como se anticipaba, la satisfacción podrá consistir en "*un reconocimiento de la violación, una expresión de pesar, una disculpa formal o cualquier otra modalidad adecuada*". Estas medidas se revelan especialmente interesantes en los supuetsos en que el daño se haya producido en relación al honor o imagen pública de un Estado. Si en el transcurso del combate un Estado viera violada su neutralidad o, de forma pública, resultara víctima de perfidia por un tercer Estado que, maliciosamente lo implicara en un conflicto contra su voluntad, la reparación deberá darse a través de estas medidas de reparacion. El reconocimiento de la violación por parte del Estado infractor supondría la restitución de la imagen pública del Estado que, frente a terceros y sin su consentimiento, se ha visto implicado en un conflicto armado.

7. CONCLUSIONES AL CAPÍTULO SEGUNDO.

Del estudio del origen, vigencia y contenido de la obligación internacional de DIH que resulta violada en el conflicto armado, a través de un ciberataque, pueden ofrecerse las siguientes conclusiones.

PRIMERA: El concepto restrictivo de ciberataque armado se justifica a la hora de establecer los límites conceptuales, respecto de otras actuaciones que pueden darse en la red, durante el conflicto armado. Como consecuencia de la adopción de criterios restrictivos que permitan delimitar el concepto de

426 El artículo 37 del PA I, establece la prohibición de matar, herir o capturar a un adversario valiéndose de medios pérfidos.

ciberataque armado, se podrán excluir del mismo los supuestos de hacktivismo, ciberdelincuencia, ciberterrorismo y ciberespionaje, a los que habrá que otorgar una regulación jurídica que dista de tener cabida en el DIH. Esta delimitación estricta del hecho ilícito, además, permite la delimitación de la obligación internacional que, al infringirse a través del lanzamiento de un ciberataque, puede originar la relación jurídica propia de la responsabilidad internacional.

Durante un conflicto armado podrán darse supuestos de hacktivismo en internet, en paralelo al activismo político o social que hasta ahora se producía de forma presencial o a través de otros medios de comunicación social. Sin embargo, el hecho de que esta actividad se desarrolle valiéndose de las ventajas que ofrece la red, no puede llevar a la confusión de que una actividad reivindicatoria, por intensa o incluso agresiva que sea, pueda llegar a ser un ciberataque y, aún menos, un ataque armado. En consecuencia, no serán de aplicación las normas de DIH aplicables al combate a estas actividades ni, como consecuencia de su inobservancia, se producirá, a través de las mismas, un hecho ilícito internacional.

La misma conclusión puede extraerse en relación a la posible participación de ciberterroristas en un conflicto armado internacional o no internacional. En estos casos, la aplicación del DIH, pretendida por algún sector de la doctrina tampoco puede compartirse, pues originaría una proliferación de los conflictos armados que ha de evitarse. Como ocurre con los casos de combatientes civiles, únicamente cuando los ciberterroristas pierdan su condición de no combatiente, caerán dentro de la regulación de las normas de DIH. En caso contrario y sin perjuicio de las cuestiones que serán objeto de un análisis en mayor profundidad en el Capítulo dedicado a la atribución del hecho ilícito cometido por agentes no estatales, hay que partir de la premisa inicial que distingue el terrorismo del conflicto armado internacional o no internacional. En consecuencia y, *a priori*, el terrorismo entra dentro de las actividades ilícitas, perseguibles por el Derecho interno e internacional relativo a los actos terroristas, pero cae fuera del Derecho de la guerra.

Las conclusiones anteriores pueden trasladarse, asimismo, a las actividades de ciberespionaje. El conflicto armado supondrá la realización de

determinadas actuaciones que, también, se desarrollan en tiempo de paz y que, en el contexto bélico suscitan dudas en torno a su calificación jurídica. Por este motivo, el concepto restrictivo de ciberataque armado que se proponía ya en el capítulo precedente, vuelve a justificarse. Únicamente cuando las actividades de Inteligencia, que desarrolla todo Ejército en combate, se lleven a cabo a través de medios cibernéticos, podrá tener cabida la aplicación del DIH, de modo que los equipos, sistemas o información, utilizados para la realización de dicho ciberespionaje pueden llegar a perder la protección de la que disfrutan, pasando así a convertirse en objetivos militares.

Es decir, que incluso en estos supuestos en los que la actividad cibernética se produce a la vez que el conflicto armado, únicamente en estos específicos y escasos supuestos será de aplicación el DIH relativo a los métodos de combate.

Las conclusiones precedentes serán de aplicación, con independencia de que nos encontremos ante un conflicto que se libre exclusivamente a través de métodos de combate cibernéticos o bien, cuando se produzcan ciberoperaciones, en paralelo a otras operaciones militares en las que se emplee otro método de combate. Asimismo, el DIH será de aplicación a los ciberataques que sean potenciadores de un conflicto armado. En todos estos supuestos será necesario discernir entre las actividades cibernéticas que quedan al margen del DIH y los ciberataques como método de combate, que exigen la observancia de las limitaciones que impone el DIH, a todos los métodos de combate.

SEGUNDA: Un ciberataque armado durante el conflicto podrá constituir un hecho ilícito continuado, con mayor probabilidad que cuando se utilzan otros métodos de combate. La ilicitud del hecho que se produce como consecuencia de la utilización de un método de combate prohibido por el DIH se extenderá durante todo el período en el que el hecho continúa y mientras se mantenga su falta de conformidad con la obligación internacional. Cuando el hecho ilícito se produce a través de un ciberataque armado, esta premisa ha de ser aplicada de forma que, en el caso de que un virus, de forma constante, afecte a la

operatividad de determinadas redes o sistemas de otro Estado, podrá ser considerado un hecho continuado.

A pesar de que los ejemplos que se recogen en el Comentario al Proyecto pudieran parecer lejanos, conceptualmente, a la consideración de los ciberataques, nada impide que la introducción de un virus informático sea considerada un hecho continuado. De esta forma, en cualquier momento en que se detecte la actuación de un ataque informático, prohibido por el DIH, podrá invocarse la violación de la correspondiente obligación. La utilización de ciberoperaciones en el conflicto armado producirá los efectos del hecho continuado con mayor frecuencia que en la utilización de otros métodos de combate. La constatación del virus Stuxnet y los efectos que el mismo produjo hacen pensar en la posibilidad de que, en el futuro, se produzcan ciberoperaciones similares. Es decir, que un ciberataque armado en el conflicto, en numerosas ocasiones, impedirá su detección en el momento preciso en que el ataque se produzca. Antes al contrario, parece más efectivo el uso de ciberataques que impidan su detención y que permitan extender sus efectos, de forma indetectable, durante el mayor tiempo posible. Por esta circunstancia, el hecho ilícito continuado será de mayor probable comisión que cuando se utilicen otros métodos de combate.

Como consecuencia de esta conclusión, la ilicitud de la conducta del hecho continuado se producirá, pues, desde el lanzamiento de una ciberoperación, que viole una norma de DIH, hasta que deje de producirse dicha violación.

TERCERA: Será ilícito el ciberataque que, en el conflicto armado, viole la obligación de la necesidad militar. El concepto de ciberataque que se defiende partiendo de unos criterios restrictivos queda todavía más limitado al aplicar los principios ineludibles de DIH relativos al combate. Las limitaciones impuestas por el DIH suponen, en primer lugar, que el ciberataque armado, en el conflicto, responda a una necesidad militar.

La licitud del ataque informático dependerá, por lo tanto, de que se produzca como consecuencia de la necesidad de conseguir un objetivo militar, de

forma que el ataque contribuya directamente al combate. Será, por lo tanto, un método de combate prohibido por el DIH el ciberataque armado que, en el conflicto, carezca por completo de esa necesidad porque no reporte ninguna ventaja militar a quien realiza el ataque.

Esta norma, aplicable a todo método de combate, cobra aquí una especial relevancia, habida cuenta la asimetría que presentan los conflictos más recientes. La disparidad de medios entre las Partes combatientes origina un desigual empleo del armamento, en función de las posibilidades reales de cada una de esas Partes. El uso del armamento informático podrá, entonces, hacerse valer para suplir las carencias en otros métodos de combate de mayor coste o de más difícil obtención. Sin embargo, el empleo de los ciberataques, por la Parte en el conflicto que cuente con menor capacidad militar, no puede justificar un empleo que no responda a la necesidad militar del ciberataque, aunque el mismo constituya una de sus escasas posibilidades ofensivas. Además, habrá que tener en cuenta aquí que, precisamente, la aparición del armamento informático contribuye a la asimetría de forma que, no puede aceptarse que el desequilibrio presente en los medios militares se corresponda, además, con un tratamiento jurídico distinto de los combatientes, en función de sus capacidades. Por lo tanto, la necesidad militar será una limitación exigible a todo combatiente y cuya inobservancia implicará la prohibición de este método de combate.

CUARTA: Es contrario al DIH y, por lo tanto, un método de combate prohibido por el mismo, el ciberataque armado que no distinga entre civiles y militares. El hecho de que nos encontremos ante un método de combate tan peculiar, no releva a los Estados en combate de su obligación de otorgar la necesaria protección a las personas y bienes civiles e impedir cualquier ataque de sus Fuerzas Armadas sobre éstos. El uso de internet como método de combate implica, nuevamente, tener en cuenta una circunstancia específica porque será especialmente difícil discernir entre las redes de uso civil y las de uso militar. En relación al personal civil protegido, tendrá esta consideración todo el que, manifiestamente, no participe en el combate. Por lo tanto, cualquier ataque a los

mismos estará prohibido por el DIH. Sería éste el caso, por ejemplo, de ataques informáticos que afectaran al sistema sanitario y, por lo tanto, repercutieran directamente en personas ajenas al combate. Asimismo, podría darse el caso de interrupción de comunicaciones o, incluso, de medios de transporte civiles que podrían ver comprometida su seguridad, a través de una disfunción en sus sistemas informáticos. Como ocurre en todo conflicto armado, el personal civil gozará de su estatuto de no combatiente. En consecuencia, si este personal entra en combate, perderá su protección, en el momento en que resulte un participante directo en las hostilidades. En el ámbito de los ciberataques podemos, además, encontrarnos con situaciones intermedias, que son específicas del manejo de ciberarmas. Así, el personal, por ejemplo, encargado de descifrar determinados códigos o programas informáticos, ha de entender alterado su estatuto y, en consecuencia, podrán ser objetivos lícitos en un ciberataque.

No obstante, hay situaciones en las que el principio de distinción es aplicable a los ciberataques de forma sencilla, como el supuesto en que, por ejemplo, el objetivo militar sea un sistema de control aéreo militar y el ciberataque produzca la imposibilidad de transporte o una alteración en el mismo.

En consecuencia, es necesario, promover un adiestramiento adecuado que permita conocer que el ataque a las redes civiles o que, de algún modo previsible, pueda tener efectos en personas o bienes civiles estará prohibido por el DIH.

QUINTA: El ciberataque armado que sea desproporcionado con la ventaja militar o que cause daños innecesarios será un método de combate prohibido. La observancia de la proporcionalidad, que prohíbe el uso la fuerza en un grado superior al necesario para el cumplimiento del objetivo militar, se aplica a los ciberataques en el conflicto armado. En consecuencia, los ciberataques deberán ser objeto del mismo examen que el resto de los métodos de combate. Precisamente, en el empleo de este método de combate, el análisis de los daños previsibles tendrá que realizarse con mayor cuidado, pues la propagación de un virus informático no siempre podrá controlarse por parte de quien lo instala.

Por otra parte, la posibilidad de seleccionar el objetivo e, incluso, de programar sus efectos en el tiempo harán de los ciberataques un método de combate, preferible a otros, en muchas ocasiones. En los casos en que se pretenda la desactivación de un objetivo militar, podrá ocurrir que esta desactivación se produzca, a través de este método, con preferencia a la destrucción física del objetivo. Es decir, en el caso que antes se exponía, en relación a los transportes militares o a la desactivación de un arma de la Parte contraria, el lanzamiento de una ciberoperación podría constituir un método de combate más eficiente y proporcionado que el bombardeo de las instalaciones o arsenales de la otra Parte combatiente. La posibilidad de minimizar los daños materiales y, sobre todo, personales, podrán, pues, aconsejar el uso de este método de combate con carácter preferente frente a otros, únicamente si, de este modo, se cumple con la obligación de observar la proporcionalidad.

SEXTA: El ciberataque, lanzado empleando la perfidia, es un método de combate prohibido por el DIH. En consecuencia, cuando en el desarrollo del combate, se ataquen redes pertenecientes a entidades especialmente protegidas con el objetivo, por ejemplo, de transmitir información de contenido militar, se estará violando esta obligación de DIH. Las actuaciones que son enumeradas en el PA I, bien podrían realizarse por medios informáticos. Es decir, que no puede restringirse la prohibición de perfidia a aquellos supuestos en los que se actúe, únicamente, a través de métodos de combate tradicionales o en los que se exija una intervención física. La propia terminología del DIH, en ocasiones, puede llevar a una conclusión errónea, al presuponer una intervención física. Sin embargo, nuevamente, es necesario dar al DIH una interpretación en función de la posibilidad de cometer esas mismas conductas a través de un ciberataque armado.

En consecuencia, los resultados que se consiguen a través de un acto pérfido, cuya comisión prohíbe el DIH, están, asimismo, prohibidos cuando se utilice internet como método de combate. Las posibilidades que internet permite, ligadas a la consecución tanto de daños personales como materiales permiten

alcanzar esta conclusión. Además, no puede olvidarse que, precisamente, la ocultación de la identidad en la red y el enmascaramiento de la misma favorecerán la adopción de comportamientos pérfidos. En este caso, pues, no sólo ha de aplicarse la prohibición de la perfidia, sino que, además, habrá que tener un especial cuidado en evitar el abuso de la buena fe de un adversario. No puede descartarse, por lo tanto, que se produzca un engaño virtual, haciendo creer a la otra Parte en conflicto que se tiene derecho a protección, cuando ello no sea así. En consecuencia, deberá quedar claro que el engaño que, fácilmente permite la red podrá caer dentro del concepto de perfidia, de igual modo que ocurre con otros métodos de combate.

SÉPTIMA: El ciberataque armado que no respete la neutralidad de terceros es un método de combate prohibido. De nuevo nos encontramos con una limitación de los métodos de combate que, pese a implicar una dificultad adicional en las ciberoperaciones, no impide su aplicación. El método de combate cibernético implica que nos encontramos en un espacio que no es físico, sino virtual y global y, por lo tanto, resultará difícil determinar la ubicación de las fronteras del Estado que se declara neutral. En consecuencia, será necesario recurrir a criterios como la localización del IP desde el que se lanza el ataque o al lugar físico en el que se produzcan los efectos del mismo. De manera evidente, estos criterios resultarán insuficientes, en ciertos casos. En todo caso, la presunción en relación con el uso de la ciberinfraestructura del Estado neutral, que propone una parte de la doctrina internacionalista, no puede tomarse más que como un mero indicio, que, en modo alguno, es suficiente, por sí mismo, para acreditar la violación de la neutralidad.

Por otra parte, esta obligación impone a los Estados neutrales la imposibilidad de realizar ciberactividades de apoyo a las acciones militares de uno de los beligerantes, en detrimento de la otra parte del conflicto. Además, los Estados neutrales estarán obligados a tomar las medidas apropiadas para poner fin al uso malicioso, por parte de los beligerantes, de la infraestructura cibernética situada en su territorio. En este caso, las conclusiones alcanzadas en

relación al hecho ilícito continuado, vuelven aquí a cobrar relieve, pues podría suceder que el uso de la ciberinfraestructura neutral se lleve a cabo sin el conocimiento del Estado neutral. En tal supuesto, el Estado neutral estará obligado a poner fin al uso ilícito, desde el momento en que tenga conocimiento del hecho ilícito que se está produciendo y durante todo el tiempo en que el mismo se realice.

OCTAVA: El contexto bélico en el que se produce la violación de DIH por un ciberatauqe utilizado como método de combate condicionará la aplicación de las medidas de reparación.Las medidas de reparación del hecho ilícito que prevé el Proyecto no pueden desligarse del método de combate que, en cada caso, queda prohibido. En consecuencia, el modo de exigir el cumplimiento de la obligación de reparar, tiene ir dirigido a conseguir la efectividad de la reparación.

Cuando la ilicitud del hecho se cometa utilizando un método de combate prohibido, la reparación no puede basarse en los mismos criterios que si dicho ilícito se hubiera producido violando otra norma de Derecho Internacional, en un contexto distinto del conflicto bélico. Ambos factores, la presencia del conflicto y la violación de una norma de DIH serán, pues, determinantes a la hora de exigir la consiguiente reparación.

Por ese motivo, en coherencia con la previsión de las medidas de reparación que establece el Proyecto, ha de tenderse, en primer lugar, a la cesación de la violación, con carácter inminente y primordial respecto de otras formas de reparar.

En el transcurso de un combate la reparación económica del daño, no puede ser prioritaria. La cesación en la comisión del hecho ilícito será la primera medida de reparación, debido a la índole del conflicto. Si, por algún tiempo, se dejara de perseguir la utilización de métodos de combate prohibidos, se producirían una serie de consecuencias que dañarían gravemente el respeto a la legalidad internacional. La primera de ellas es que, de forma previsible, se estaría fomentando la asimetría en el conflicto.

Esta asimetría se manifiesta, cada vez más, como consecuencia de la desproporción de capacidades militares entre las Partes combatientes, pero no puede tener su reflejo en el ámbito jurídico. Por el contrario, la exigencia del cumplimiento del DIH en el combate ha de ser idéntica respecto de todas las Partes combatientes. De este modo, incluso, en los supuestos en que el Estado agresor esté en condiciones de reparar, finalmente, el perjuicio causado, seguirá obligado a cumplir con la obligación violada. En los conflictos armados en los que se lancen ciberataques prohibidos por el DIH, tendrá que exigirse su cese, tan pronto como se tenga conocimiento de la ilicitud del hecho. Nos encontramos en un contexto en el que, de otra manera, el Estado agresor podría lograr una ventaja militar que, posteriormente, dejara sin efecto cualquier otra medida de reparación. En el caso de que se estuviera violando, por ejemplo, la obligación de distinguir entre objetivos civiles y militares, atacando la red sanitaria civil, el cese deberá ser inminente para evitar la producción de bajas. Lo mismo cabe decir del ciberataque que cause daños innecesarios o desproporcionados. En definitiva, no podrá permitirse la actuación de un Estado en combate que, ante su inferioridad en otras capacidades militares, decida valerse de su superioridad en medios informáticos, si estos no son utilizados de forma lícita. Antes bien, la obligación de respetar y hacer respetar el DIH ha de exigirse en todo momento del conflicto armado, sin que la inferioridad militar de una de las Partes pueda tomarse como justificación para eludir dicho cumplimiento.

Como consecuencia de lo anterior, si la Comunidad Internacional no reaccionara en ese sentido o el Consejo de Seguridad de Naciones Unidas, no calificara como ciberataque armado un ataque que realmente lo fuera, se pondría en serio peligro la seguridad jurídica internacional.

Por otro lado, puede, además, afirmarse que la existencia de un daño material o moral no es un requisito imprescindible para el surgimiento de la responsabilidad internacional del Estado, derivada de la utilización de un método de combate, prohibido por el DIH. La responsabilidad del Estado constituye una relación jurídica nueva, distinta de la que ha sido violada, con independencia de la existencia o no de un daño físico o moral que, únicamente,

se tendrá en cuenta a la hora de hallar el modo más efectivo de reparar el perjuicio sufrido. Ello no impide, lógicamente que, cuando esos daños sean acreditados, la reparación tenga que ser íntegra y cubrir la producción de todo el perjuicio sufrido, cualquiera que sea la índole del mismo, material o moral.

Surge aquí otra de las características propias de la producción del hecho ilícito como consecuencia de la utilización del ciberataque como método de combate. Con carácter general, la acreditación de los daños implica la reposición al Estado lesionado, en la situación previa a la infracción, siempre que no sea materialmente imposible. Pues bien, esta imposibilidad se dará, previsiblemente, cuando se utilicen los ciberataques como método de combate, debido al efecto multiplicador que puede alcanzar un virus, al originar la infectación de múltiples equipos informáticos en muy poco tiempo, si se pierde el control sobre su propagación y efectos.

Sin embargo, la principal limitación en el momento de obtener la reparación del daño causado se originará por parte del propio Estado lesionado, pues la acreditación de los daños producidos no siempre será conveniente para el Estado que los sufre. En este específico ámbito, esta acreditación equivaldrá a poner en evidencia las vulnerabilidades de la red, con el riesgo que ello puede suponer, en el desarrollo del combate. Asimismo, como consecuencia del ciberataque ilícito, podría producirse la pérdida de información o de datos que el Estado lesionado no tenga interés en desvelar. Si, por ejemplo, hubiera que reparar un daño producido como consecuencia de un ciberataque pérfido, no siempre será conveniente para el Estado que ha sufrido el engaño en la red, desvelar en qué modo el Estado agresor ha causado dicho engaño.

En consecuencia, la reparación del daño, aun cuando sea posible, podrá no ser conveniente para el Estado lesionado, de manera que el mismo tendrá que acudir a las medidas reparadoras consistentes en la prestación de seguridades y garantías, Por otra parte, estas medidas no pueden contemplarse únicamente de forma subsidiaria, es decir, a falta de efectividad de las anteriores, sino de modo principal en los casos en que el ciberataque sufrido lo exija. Si volvemos al caso de los ataques sufridos por Estonia y la paralización del teléfono de emergencias,

se manifiesta la necesidad de que, en un ciberataque armado durante el conflicto, que infrinja la obligación de distinguir entre objetivos civiles y militares, la cesación será la medida prioritaria a adoptar. Como segunda medida se presenta esencial el aseguramiento y la prestación de garantías de que dicho ciberataque no va a volver a producirse. En estos casos, pues, la reparación posterior del daño económico podría exigirse, pero, evidentemente, su finalidad reparadora quedaría mermada sin las medidas anteriores.

La previsión del Proyecto de las medidas reparadoras contempla, asimismo, la posibilidad de exigir indemnización al Estado infractor. En el caso de que el hecho ilícito se cometa a través de un ciberataque contrario al DIH, esta medida podría contemplarse, a falta de satisfacción obtenida, aplicando las anteriores, pero presenta las mismas dificultades que las descritas anteriormente. Cualquier evaluación económica puede encontrarse con los problemas antes citados, en relación con la reparación de daño y a éstas hay que añadir que, el principal daño en el combate serán las bajas humanas. Si estas bajas se producen, como consecuencia del empleo de un método de combate prohibido, la indemnización, con toda seguridad, será tan ineficaz como cualquier otra medida económica.

Por este motivo, además, resulta especialmente interesante la última posibilidad que ofrece al respecto el Proyecto de artículos, al contemplar las medidas de satisfacción. En el caso que antes se citaba del lanzamiento de un ciberataque pérfido, parece evidente que el descrédito producido al Estado, a través del engaño, debería ser objeto de reparación, a través de las medidas de satisfacción. Pero, además, es evidente que, a través del engaño, el Estado infractor, podría hacer creer a la Comunidad Internacional o a terceros ,que el Estado lesionado participa en un conflicto armado, de forma que el Estado víctima del hecho ilícito podría ver perjudicada su imagen u honor.

Igualmente ocurriría en el caso de violación de la neutralidad. Si la ciberinfraestructura de un Estado neutral fuera utilizada sin que de dicho Estado tuviera ocasión de impedirlo, los daños al mismo serían evidentes. La participación en un conflicto internacional, prestando ayuda o asistencia a un

tercero, aun de forma involuntaria, podría perjudicar enormemente a un Estado en sus relaciones con terceros Estados y desacreditar su imagen ante la Comunidad Internacional. Si, posteriormente, se probara que el Estado neutral fue víctima de un ciberataque prohibido por el DIH, parece que la medida de reparación más adecuada consistiría en la satisfacción. A través de la misma, el Estado lesionado debería exigir la aceptación del hecho ilícito por parte del Estado infractor, las consiguientes disculpas y la reposición de su imagen ante la Comunidad Internacional, terceros Estados o sus aliados.

CAPÍTULO TERCERO. LA ATRIBUCIÓN DEL HECHO ILICITO CAUSADO POR EL LANZAMIENTO DE UN CIBERATAQUE COMO MÉTODO DE COMBATE.

1. INTRODUCCIÓN.

Una vez analizados los requisitos que según el DIH resultan necesarios para la comisión del hecho ilícito por acción u omisión, corresponde el estudio de las consecuencias de dicho ilícito. La primera consecuencia será que no podrá darse responsabilidad internacional del Estado si no es posible atribuir ese hecho ilícito a determinados sujetos de Derecho Internacional, contemplados en el Proyecto.

En el presente trabajo, se abordará la responsabilidad del Estado y, en consecuencia, será necesario atender a los casos en que el hecho ilícito le sea atribuible. Para ello será preciso acudir, en coherencia con la sistemática hasta ahora empleada, al régimen de DIH Convencional y consuetudinario, así como a las previsiones que el Proyecto realiza al respecto, sin olvidar la Jurisprudencial Internacional. Sin embargo, se abandonará el esquema hasta ahora seguido, de forma tal que no todos los supuestos recogidos en el DIH consuetudinario y en el Proyecto, van a ser atendidos, por cuanto, de no todos ellos puede predicarse la misma importancia en relación a la atribución. Es decir, la Compilación de DIH consuetudinario, establece en su Norma 149[427] que

> «*Un Estado es responsable de las violaciones del DIH, en particular:*
> *a) las violaciones cometidas por sus órganos, incluidas sus fuerzas armadas;*
> *b) las violaciones cometidas por personas o entidades autorizadas a ejercer prerrogativas de su autoridad gubernativa;*
> *c) las violaciones cometidas por personas o grupos que actúan de hecho obedeciendo sus instrucciones o bajo su dirección o control; y*
> *d) las violaciones cometidas por personas o grupos privados que él reconoce y acepta como comportamiento propio*».

427 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; pp. 599-606.

La antedicha Norma, resulta aplicable a las violaciones cometidas tanto en los conflictos armados internacionales como en los no internacionales. Pues bien, como podrá verse en el desarrollo del presente Capítulo, determinadas situaciones que la norma cita, no suscitan interés en relación a la atribución de la conducta, mientras que otras que, parecen estar previstas para situaciones excepcionales o minoritarias, deberán ser objeto de especial atención, pues constituirán la práctica más frecuente en los conflictos en los que interviene el elemento cibernético.

Así, este tercer capítulo comienza con la exposición de las específicas cuestiones que, en relación a la atribución van a presentarse en los supuestos de ataques informáticos.

Es decir, a tenor de lo dispuesto en el proyecto, no puede haber responsabilidad del estado si no hay un hecho ilícito que sea atribuible a dicho Estado. Pues bien, en el caso de los ataques informáticos, el anonimato y la ocultación de la identidad se dan con una gran frecuencia, hasta el punto de que en muchas ocasiones resultan consustanciales al uso de este elemento. De esta característica han de extraerse distintas consecuencias.

La primera de ellas es la constatación del brusco giro en la forma de combatir, pues, tradicionalmente, las acciones de guerra eran atribuidas a un Estado, por el propio interés del Estado, que no solía mostrar interés en ocultar la autoría. En la actualidad, sin embargo, como se verá en el segundo epígrafe, las posibilidades de enmascarar la autoría de los ciberataques son múltiples y se encuentran a disposición tanto de los Estados como de los agentes no estatales. Será preciso, entonces, atender a estas cuestiones que pudieran parecer de índole más técnico pues, a pesar de no ser el objeto del presente trabajo de investigación, es lo cierto que no puede omitirse una referencia, aun breve a estas cuestiones materiales, en tanto que condicionan los aspectos jurídicos que será tratados en el epígrafe siguiente. Por último, en estrecha relación con lo anterior, se hará alusión a la necesidad de lograr una eficaz cooperación entre el sector público y el privado que permita de lograr una auténtica cultura de ciberseguridad y cubrir, así, las lagunas que se constatan para Estados y particulares.

Una vez analizados los retos de carácter material que la atribución presenta, será momento de iniciar el estudio de los dos grandes bloques de agentes que podrán encontrarse en el desarrollo de un conflicto armado: el Estado y los agentes no estatales. En ambos casos, las conclusiones extraídas en el epígrafe precedente, en relación a las dificultades de indagación de autoría, deberán tenerse presentes, pues las posibilidades técnicas descritas en el citado epígrafe se encontrarán a disposición de ambos tipos de sujetos.

En el supuesto de la actividad de Estado, resulta especialmente relevante la actuación de los miembros de las Fuerzas Armadas. Convienen, en este punto tener en cuenta que, el presente estudio tiene como objeto la realización de un hecho ilícito a través del uso de internet como método de combate y, por lo tanto, de forma ineludible tendrá que atender a la responsabilidad del Estado, como consecuencia de la actuación de sus militares, pues éste será el caso más frecuente, en el ámbito que aquí se analiza. Por ello, este aspecto de la responsabilidad estatal, que en otros ámbitos pudiera parecer excepcional o incluso tangencial, cobra aquí una dimensión sustancial. Por otra parte, como ya se ha adelantado en la parte primera del presente trabajo, la disponibilidad de los medios informáticos y la novedad en el manejo de los mismos, exige tener presente que su uso no siempre va a realizarse de un modo completamente adecuado. Por tal motivo, se verá con especial detenimiento la doctrina relativa a los actos llamados *ultra vires* cuando éstos sean cometidos por miembros de las Fuerzas Armadas.

Por último, el epígrafe hará referencia a los supuestos de colaboración entre Estados para el lanzamiento de un ciberataque y, en consecuencia, se analizará con especial atención el contenido del artículo 16 del Proyecto. Dicho análisis se entiende necesario en atención a la especial complejidad técnica que se ha constatado en algunos de los virus informáticos más recientes, por cuanto la misma presupone una colaboración entre distintos agentes, a la hora de desarrollar la herramienta informática y de lanzar el ciberataque. Por ello, la delimitación de responsabilidades entre los Estados que cometen por sí mismos el ilícito y la de los Estados que proporcionan la ayuda o asistencia necesaria para

poder realizarlo tendrá que ser realizada teniendo en cuenta los especiales componentes de este método de combate.

La atribución del hecho ilícito plantea problemas, asimismo, relacionados con otros agentes intervinientes en un conflicto armado. Por ello, al margen de los Estados, habrá que hacer mención específica a los agentes no estatales que puedan estar presentes en el combate. La presencia de agentes no estatales en el conflicto armado no es nueva, pero se presenta aquí bajo una nueva apariencia que habrá que estudiar desde distintas perspectivas y, como se viene haciendo, a la luz del DIH convencional y consuetudinario. La utilización de agentes no estatales por parte de los Estados, ha sido puesta en evidencia por algunos autores de la doctrina internacionalista que han denunciado, incluso, la ventaja implícita a dicha práctica que consiste en la imposibilidad de atribución del hecho ilícito al Estado y, en consecuencia, la inexistencia de responsabilidad internacional[428].

En este sentido, de todas las previsiones que realiza el Proyecto de artículos, resulta especialmente relevante la atinente a los agentes no estatales que desempeñan atribuciones del poder público siempre que, esa persona o entidad, actúen en el ejercicio de dicha capacidad. De este modo, nos podremos encontrar con dos tipos de agentes no estatales, las corporaciones mercantiles de capital privado o público y los particulares que, a título individual o formando parte de un grupo, intervienen a través de la red en un conflicto armado internacional o no internacional. La relevancia de esta cuestión radica, esencialmente en el hecho de que supone una excepción a la regla general en virtud de la que el uso de la fuerza constituye una competencia que el Estado ejerce en monopolio. Es decir, de forma evidente, en el supuesto de un conflicto armado internacional, la conducción de las hostilidades en el caso de será desarrollada por las Fuerzas Armadas de los Estados en combate. Sin embargo,

428 PADMANABHAN ofrece el reciente ejemplo de la utilización de agentes no estatles en el conflicto entre Rusia y Georgia, al expresar que: "*For example, the Georgian government accused the Russian Federation of hiring criminal organizations and encouraging patriotic "hacktivists" to launch attacks against Georgia during the 2008 conflict over South Ossetia*". PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*. US Naval War College. International Law Studies, vol. 89, 2013; pp. 288-307.

en la actualidad dicha regla general quiebra desde el momento en que determinados agentes no estatales están presentes en los conflictos, hasta el punto de que sea necesario valorar si dicha presencia puede tenerse por la participación directa en las hostilidades[429].

En el primer caso, a su vez, será necesario abordar la cuestión de la aplicabilidad del DIH en dos supuestos distintos, constituidos por la presencia de las empresas privadas, propietarias y gestoras de redes informáticas de las que se vale en el Estado y, en concreto las Fuerzas Armadas en combate y, en segundo lugar, el papel a desarrollar por las empresas que, igualmente son propietarias y gestoras de entes que quedan englobados en alguno de los sectores que componen las infraestructuras críticas del Estado.

En ambos casos, habrá que delimitar la responsabilidad de quien actue al mando de dichas empresas, bien propiciando un ataque, bien en respuesta a uno que se haya sufrido. Dicha delimitación vendrá condicionada por la naturaleza de la misma red que, como se hizo constar en el Capítulo precedente, es susceptible de un doble uso civil y militar[430].

Con posterioridad se analizará el papel que los ciber voluntarios puede desarrollar durante un conflicto armado, ya sean éstos parte de una organización o, por el contrario, actúen de modo individual. En el primero de los casos se hará

---

429 Así lo entiende también LOBEL que, en este sentido, afirma: "*The state's monopoly on the use of force serves a key function in law of war compliance. The problem in the context of the private sector and cyber conflict is two-fold. First, the rules themselves are unclear. Second, the private sector lacks the kind of organizational structure and institutional competence that facilitates compliance with law of war rules. Cyber conflict is a new war domain, with unique obstacles to applying existing norms. Private entities face the same fuzzy rules, but have no background in the law of war or experience in armed conflict upon which to draw. More importantly, a private entity's primary motivation is likely not national security but rather the corporate bottom line. The private sector might not only erode the state's monopoly on the use of force, but also use that force in service of ends that do not serve the public interest*". LOBEL, H. *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict.* Texas International Law Journal, vol. 47, issue 3; pp.638-639.

430 Entre otros, RATTRAY y HEALEY, han expuesto esta dificultad de delimitación del uso público y privado de la red: "*In cyberspace, there is no analogous empty "space" and the activities of civil and military users are intertwined together. Non-state actors cannot flee the domain since cyberspace is composed of technologies, software and hardware overwhelmingly created, owned and operated by non-state commercial actors with their own capital and for their own reasons. Global fiber optic networks, tier I Internet service providers (ISPs) and large commercial web hosting companies will be the battlespace for many or most conflicts, and they cannot evacuate the battlefield except by unplugging and dismantling part of cyberspace itself*". RATTRAY, G. J. AND HEALEY, J. *Non -State Actors and Cyber Conflict. America's Cyber Future.* Security and Prosperity in the Information Age. Center for a New American Security, vol. II. June 2011; pp.65-86, en particular, p.67.

una especial mención a los supuestos de ciberterrorista, tan presentes en la red y al modo en que han de ser calificadas y tratadas jurídicamente sus actuaciones. La distinción entre el ciber terrorismo y el conflicto armado que se expuso en el capítulo recedente, ha de traerse de nuevo colación a la hora de determinar si a los ciber terroristas que actúan simultáneamente al desarrollo de un conflicto armado, les es de aplicación el DIH o, por el contario sus ciberataques terroristas han de someterse al Derecho Penal interno o internacional.

Por otra parte, la entrada en combate de individuos que no forman parte de las Fuerzas Armadas de una Parte combatiente pondrá asimismo en evidencia la necesidad de reconsiderar las teorías que hasta ahora han sido manejadas en relación con la atribución. Ya se ha llamado la atención en la Primera parte del presente trabajo sobre la evolución de la manifestación de los actuales conflictos y sobre la extensión de una nueva tipología de los mismos que incluye y, en ocasiones prioriza, el llamado conflicto híbrido. Será en este contexto donde la aparición de cibercombatientes, que toman parte por una de las Partes del conflicto, sin formar parte de ella, haga necesario el replanteamiento de determinadas construcciones jurídicas hasta ahora empleadas.

Estos ciber combatientes deberán ser examinados a la luz del DIH y de la Jurisprudencia Internacional para determinar si nos encontramos ante una situación realmente novedosa o por el contrario, ante una nueva modalidad de participación en el combate por parte de personal civil. Resultará aquí de especial relevancia, en primer lugar el estudio de las doctrinas relativas al control del Estado en relación con los actos de los agentes no estatales, en orden a la atribución del ilícito a dicho Estado. En este sentido, la Jurisprudencia internacional aportará los elementos necesarios para establecer un criterio en el contexto de los ciberataques. Así, tomando como punto de partida las teorías relativas al control efectivo y al control general que se han aplicado en distintas decisiones por la Jurisprudencia internacional, se estudiará el modo en que los participantes en los conflictos armados, a través de la red pueden ser considerados o no agentes del Estado, de modo que sea éste y no los individuos, el que responda internacionalmente por el hecho ilícito cometido.

Asimismo, resulta imprescindible en el estudio de estas cuestiones, nuevamente, el análisis del DIH convencional y consuetudinario, así como el de los criterios expuestos por el CICR en relación a la doctrina de la participación directa en las hostilidades, pues únicamente en aplicación de la misma se podrá vislumbrar si esta nueva modalidad de combate es susceptible de ser encuadrada jurídicamente, como una participación en el mismo. La condición de combatiente que se otorgue a estos voluntarios que actúan a título individual o de modo organizado, tendrá las consecuencias jurídicas que el DIH prevé, en relación a la calificación de sus actos y con la protección que deba serles otorgada, en caso contrario, como personal civil. En definitiva, deberá plantearse si la participación de cibervoluntarios en el conflicto armado, permite que éstos sean tomados como objetivo militar o no y si las acciones de los mismos son atribuibles a un Estado o no.

Sin embargo, la particular idiosincrasia de los atacantes que en la realidad se están constatando justifica que, en el estudio de estos aspectos se abandone el esquema planteado por el Proyecto de artículos, pues, la realidad demuestra que las situaciones relativas a los ciber voluntarios distan lo suficiente de las planteadas en el Proyecto, como para atenderlas de modo específico.

En este sentido, la doctrina internacionalista más reciente ha abordado la atribución al Estado de los ciberataques entendiendo que la misma responde, esencialmente a la construcción que dicha relación jurídica presenta en el Proyecto de artículos, puntualizando que un hecho ilícito, cometido a través de un ciberataque puede consistir en la violación de la Carta de Naciones Unidas o de las normas de DIH, sin que la causación de un daño sea requisito ineludible para la exigencia de dicha responsabilidad[431]. No obstante, la cuestión de la atribución al Estado, como se verá en el presente Capítulo, entraña la compleja tarea de determinar en qué casos, un Estado se halla tras el lanzamiento de un ciberataque que, de forma frecuente va a ocultar su autoría.

431 Así está contemplado en la Norma 6 del Manual de Tallín.SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; pp.29-34.

Esta reciente doctrina ofrece, en este ámbito, una serie de presunciones que aplicables a la hora de regir la atribución al Estado de los ciberataques cuya autoría no resulte claramente determinada. Así, el Manual de Tallin entiende que el criterio del lugar en el que se produce el ataque o donde se localizan los civervoluntarios, no ha de afectar necesariamente a la determinación de la responsabilidad del Estado. Así lo afirma su Norma 6, ya citada que parece pretender el objetivo de descartar criterios de atribución erróneos. En efecto, puede compartirse con los autores que los criterios hasta ahora empelados pueden originar atribuciones erróneas en esta materia, pues la facilidad con la que, como se verá, puede ser ocultada la autoría, podría conllevar la atribución a Estados que ninguna relación hayan tenido con el ciberataque o ciber operación en cuestión.

Sin embargo, los problemas en materia de atribución, cuando el hecho ilícito de produzca a través de la red, van a resultar un elemento esencial y determinante que exige la atención de estas cuestiones de un modo más detenido[432], sin obviar la utilidad de la aplicación de las presunciones expresadas en las Normas 6 y siguientes del Manual de Tallin. En caso contrario podría suceder que, en este ámbito, también se produjera la minoración en la exigencia de control necesario para la imputación al Estado de los actos consumados por grupos o individuos, tal como se viene constatando desde los atentados ocurridos en los Estados Unidos el 11 de septiembre de 2001[433].

En definitiva, esta dificulat de atribución al Estado de los hechos ilícitos cometidos por internet, conlleva la necesidad de abordar la aplicación de la doctrina del control de Estado, de tal modo que resulte adecuada a las nuevas

---

432 SHACKELFORD defiende asimismo esta idea: "*Attribution of a cyber attack to a State is a, if not the, key element in building a functioning legal regime to mitigate these attacks*", SHACKELFORD S. J., *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem.* Conference on Cyber Conflict Proceedings 2010 C. Czosseck and K. Podins (Eds.) CCD COE Publications, 2010, Tallinn, Estonia; pp. 197-208, en particular, p.200.

433 Así lo ha puesto de manifiesto LOBEL, al entender que "*Once a test of whether a state exercised effective or overall control over the non-state actor, the emerging standard now appears to be whether a state "harbored" or "supported" the non-state actor. Given the difficulty of technical attribution in the cyber domain, some scholars are pushing the idea that imputation standards should follow this trend in relaxation in order to lift the "veil of plausible deniability" that allows states to "escape accountability" by hiding behind private hackers*". LOBEL, H. *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, op. cit.; pp.638-639.

modalidades comisivas del hecho ilícito y sin abandonar la defensa de la teoría general de corte restrictivo que aquí se viene defendiendo[434].

2. LAS ESPECIALES DIFICULTADES EN LA ATRIBUCIÓN AL ESTADO DEL HECHO ILÍCITO COMETIDO VIRTUALMENTE.

El presente trabajo de investigación ha tenido por objeto, hasta el momento, el análisis de cómo la violación de una obligación de DIH puede constituir un hecho ilícito y, por lo tanto, originar la aparición del primer elemento necesario para la exigencia de responsabilidad internacional. De este modo, volviendo al tradicional esquema de la exigencia de responsabilidad internacional del Estado, existirá dicha responsabilidad internacional si el referido ilícito es atribuido a un Estado.

Es, en este punto, donde de modo más visible va a resultar la dificultad de exigir dicha responsabilidad al Estado, pues nos encontramos ante la producción de una serie de ilícitos, cuya autoría, difícilmente, va a mostrarse con claridad. Si, hasta ahora, se ha presentado la necesidad de la reinterpretación de determinados conceptos a través de la aplicación de un método analógico, que permita dar respuesta jurídica a una nueva realidad, en este momento, es necesario realizar una nueva conceptuación de determinados ámbitos. Esta necesidad que excede, por lo tanto, de la mera interpretación, se justifica en el hecho de que, el mantenimiento de concepciones tradicionales, pudiera llegar a impedir la exigencia de responsabilidad.

Por otra parte, a la hora de abordar la responsabilidad del Estado, por hechos cometidos por sus órganos, habrá que tener presente que, en el uso de la red, los Estados se van a beneficiar de las mismas técnicas que otros usuarios que dificulten la indagación de la autoría. A ello se une el hecho de que, como

434 LOBEL se decanta, asimismo, por un criterio restrictivo al afirmar que: "*Until the technical side of attribution develops to a point that instills confidence, the best course is to maintain a stricter standard for imputation. This better serves the goals of international law of protecting civilians from harm and suffering. It also will serve as a disincentive to those non-state actors seeking to exploit a relaxed imputation standard by pursuing "false flag" operations or other techniques that turn innocents into virtual human shields*". LOBEL, H. *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, op. cit.; pp.638-639.

manifiesta SHACKELFORD, nos encontramos con una técnica forense, todavía poco desarrollada, que no facilita la tarea de atribución que aquí se analiza[435].

Por otra parte, la participación de personal civil en los conflictos armados, a través del lanzamiento de ciberataques, ya pertenezca a empresas privadas, ya sean particulares, que actuan por su propia iniciativa, plantea la necesidad de reelaborar los conceptos que, tradicionalmente, han permitido la atribución de un hecho ilícito. Por ello, en el presente epígrafe se van a exponer las referidas dificultades, a la hora de identificar a quienes, de uno u otro modo, perpetran los ciberataques, de modo que las presentes consideraciones tendrán que tenerse en cuenta el análisis del contenido completo de este Capítulo.

En los casos que hasta ahora se han atendido, por resultar de mayor relevancia práctica, a los efectos que aquí nos ocupan, es evidente que, si algo quedó suficientemente acreditado, fue la dificultad de atribuir los ataques cibernéticos al Estado al que, de manera más probable, eran imputables. Es decir, a falta de una reivindicación expresa y pública, será muy difícil hallar el nexo de unión entre el hecho ilícito y el Estado en cuestión. Incluso en los casos en que ello ocurra, como en los ataques de índole terrorista, tampoco podrá afirmarse, sin género de duda, que la acción sea atribuible al Estado. Para algunos autores, incluso, el lanzamiento de un ciberataque, utilizando adecuadamente todas las medidas de precaución, que ofrece la técnica, permite que el autor del mismo resulte inidentificable y, en consecuencia, que la atribución se torne imposible[436].

Esta situación ha sido puesta de manifiesto en numerosas ocasiones siendo las más relevantes los ciberataques que aquí se viene citando. Así, cabe recordar la imposibilidad de identificar a los autores, que perpetraron los ciberataques que

435 Así, el autor entiende que "*The science of tracing cyber attacks is primitive at best. Sophisticated attacks by knowledgeable hackers, whether private or State sponsored, are nearly impossible to trace to their source using modern practices*". SHACKELFORD, S. J., *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, op. cit.; p.200.

436En este sentido se expresa LIN que afirma que: "*This statement does have an essential kernel of truth: if the perpetrator makes no mistakes, uses techniques that have never been seen before, leaves behind no clues that point to himself, does not discuss the operation in any public or monitored forum, and does not conduct his actions during a period in which his incentives to conduct such operations are known publicly, then identification of the perpetrator may well be impossible*". LIN, H., *Cyber conflict and international humanitarian law*. International Review of the Red Cross. Humanitarian debate: Law, policy, action. New technologies and warfare, vol. 94, no. 886, Summer 2012; pp.515-531, en particular, p. 522.

sufrió Estonia en el año 2007[437]. Fue éste el primer supuesto que, con cierta relevancia pudo constatarse, en relación a un Estado, que es atacado a través de internet y, por ese motivo, del mismo, debieran extraerse las correspondientes lecciones aprendidas, a la hora de abordar el resto de supuestos. Puede decirse que los hechos, a los que los dirigentes de Estonia hubieron de hacer frente, no fueron especialmente graves porque el clima social que, en ese momento, existía en el país, pese a ser delicado, no llegaba a rebasar el umbral de violencia, requerido para poder hablar de un conflicto armado. Sin embargo, un supuesto muy similar pudo comprobarse, en el caso de los ataques sufridos por Georgia, con la circunstancia añadida de que, dicho Estado sí se hallaba librando un conflicto armado y de que, los ataques informáticos se sucedieron, desde el mismo momento, en que estalló el conflicto[438]. En ambos casos, la atribución de dichos los ciberataques fue prácticamente imposible y, en el caso de Georgia, incluso se especula sobre cuál de las dos Partes del conflicto, comenzó los ciberataques[439]. Asimismo, hace constar que no hay ningún tipo de prueba sobre que Rusia estuviera involucrada en dichos ataques. De igual modo, quedó constatada la imposibilidad de averiguar la identidad la identidad de quienes perpetraron los ataques informáticos y, si bien Georgia responsabiliza a Rusia de dichos ataques, Rusia declina cualquier responsabilidad[440].

En este momento tambien es necesario volver al estudio de otro de los ataques informáticos que, por sus circunstancias y naturaleza, han resultado hasta la fecha, paradigmáticos. En el caso de la introducción del virus Stuxnet en la central nuclear iraní, el hecho de que, únicamente de forma vaga y sin pruebas

437 Así ha sido señalado por TIKK, al afirmar que "*Combining the complications discussed above with the restriction regarding issuing international requests for assistance (as this measure was not legally permissible in those cases where the "single inquiry" was the only surveillance activity permitted) in a situation where attacks were globally sourced from over a hundred nations, and it becomes apparent that the national legal system was not likely to do too well in identifying the perpetrators*". TIKK, E., KASKA, K., VIHUL, L., International cyber incidents: legal considerations, op. cit.; p. 27.

438 En este sentido, ALLAN afirma que "*On the evening of August 7, 2008, the tension that had been building along the Russian-Georgian border for several months reached a head, resulting in an armed conflict between Russian and Georgian Forces*". ALLAN, C.S. *Attribution Issues in Cyberspace*, Chicago-Kent Journal of International and Comparative Law, vol.13, issue 2. 2013; pp.55-83, en particular, p. 58.

439 Asi lo recoge ALLAN en la obra citada, ALLAN, C.S., *Attribution Issues in cyberspace,* op. cit.; p. 61.

440 ALLAN, C.S., *Attribution Issues in cyberspace,* op. cit.; p. 61.

materiales, haya podido especularse sobre la autoría del hecho, pone de manifiesto la especial importancia de esta cuestión[441]. Algunos autores han recogido la afirmación de que los Estados Unidos, en conjunción con Israel, pudieran haber desarrollado el virus y ser responsables de su introducción en la central nuclear de Irán[442]. Sin embargo, no ha podido ser acreditado si ello realmente fue así y, en ese caso, en qué medida, cada uno de los Estados, contribuyó al desarrollo e introducción de dicho virus[443].

Por último, hay que hacer mención al reciente caso de los ataques cibernéticos, sufridos por Ucrania, durante el desarrollo del conflicto armado internacional con Rusia. Vuelve aquí a ponerse de manifiesto cómo, durante el desarrollo del combate, se suceden una serie de ciberataques, cuya autoría y atribución constituyen una incógnita. Como STINISSEN afirma, la actividad "*maliciosa*" en el ciberespacio se desarrolló, de forma paralela a las operaciones militares en Crimea, de manera que se lanzaron operaciones, contra la infraestructura de telefonía de Ucrania, los teléfonos móviles de los miembros del Parlamento de Ucrania y las compañías de seguridad[444].

---

441 Así lo afirma ZIOLOWSKI: "*Although a cui bono analysis can perfectly well point in the direction of entities that might have an interest in affecting Iran´s nuclear programme, it does not provide sufficient indices in legal terms to attribute the malicious cyber-activity to an individual, to a group of individuals or even to a State*", ZIOLOWSKI, K. *Stuxnet-Legal considerations*. Cooperative Cyber Defense Centre Of Excellence. Tallin 2012; p.5. Documento disponible en el sitio web:https://ccdcoe.org/sites/default/files/multimedia/pdf/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf. Fecha de consulta, enero de 2013.

442 PADMANABHAN, en este sentido no tiene duda sobre la coautoría de ambos Estados:" *The United States and Israel launched a cyber operation against Iran's burgeoning nuclear program that used malicious code to im-pede the functioning of Iran's centrifuges in order to secure additional time for negotiations over the future of Iran's nuclear capability*". PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*, op. cit.; p. 289.

443 Así LIN afirma que "*the United States and/or Israel were responsible for the cyber attack on Iranian nuclear facilities (Stuxnet)*". LIN, H., *Cyber conflict and international humanitarian law*, op. cit.; p.519.

444 Por el interés que puede suscitar la cronología de los recientes hechos, se expone aquí, de forma resumida el relato que, de los mismos, realiza el citado autor: "*Before the Euromaidan protests began, tensions in Ukraine had already triggered hostile activity in cyberspace. Politically motivated hacker groups launched Distributed Denial-of-Service (DDoS) and other cyber attacks against a wide range of targets. On 28 October, the hacker group 'Anonymous Ukraine' started 'Operation Independence' (#OpIndependence), favouring Ukraine's independence from any external influence, including the EU, NATO, and Russia.6 Operation Independence included DDoS attacks and website defacements against both Western and Russian sites. During Euromaidan DDoS attacks and defacements against both sides continued. Information leaks were used for propaganda purposes. Operation Independence leaked emails from opposition leader Vitali Klitchko and his political party, the Ukrainian Democratic Alliance for Reforms. Unknown hackers leaked the U.S. officials' phone call which included the infamous statement, 'f*ck the EU it was primarily an internal matter between a state and an opposition within that state. And*

Pues bien, todos estos supuestos son prueba manifiesta de que, será en el momento de la atribución, en el que surgirán las principales dificultades, a la hora de exigir responsabilidad internacional del Estado. Esta dificultad de atribución viene facilitada por la propia naturaleza de la infraestructura que se utiliza[445] y resulta consustancial a la misma. Por este motivo, precisamente es por el que la indagación de la autoría deberá tratarse como una cuestión primordial y característica de los ciberataques.

---

while the conflict engendered considerable violence – one only has to look at the number of casualties – at that stage, it could not be seen as an 'armed conflict'. In cyberspace, there was a simultaneous rise in malicious activity during the military operations in Crimea. Operations were conducted against Ukraine's mobile infrastructure, the mobile phones of members of the Ukrainian Parliament, and security communications. Some traditional methods were used, including the seizure of Ukrtelecom offices and the physical cutting of telephone and internet cables. Digital attacks included DDoS targeting Ukrainian, Crimean, NATO, and Russian websites. The pro-Russian hacker group CyberBerkut was particularly active against NATO, while groups like OpRussia and Russian CyberCommand directed their actions against Russian websites. Polish, Ukrainian, and Russian websites were also defaced. (…) Spyware Snake (also known as Ouruborus or Turla) was used against several targets in Ukraine, including the government. Snake is sophisticated malware, known to be in use for at least eight years, whose origin is uncertain, but believed to be developed in Russia. (…) NATO reported the active involvement of Russian troops in eastern Ukraine, but Russia has consistently denied involvement. Cyber operations have continued throughout the conflict. In May 2014, cyber means were used in an attempt to disrupt the presidential elections, including an effort to falsify the outcome. (…) CyberBerkut may have taken part and some analysts believe that Russia was behind it. In August 2014, hackers conducted a DDoS attack against Ukraine's election commission website, just prior to the parliamentary polls. intelligence gathering through cyber means, all of which reportedly have a Russian connection Snake malware was employed against the Ukrainian Prime Minister's Office, as well as a number of foreign embassies. In April 2015, Lookingass reported on a Russian campaign to extract classified documents from Ukrainian military and law enforcement agencies in an effort to support pro-Russian military operations in Ukraine. ISight Partners reported that Russian Sandworm hackers used a 'zero-day' vulnerability to hack NATO and Ukraine in a cyber espionage campaign. The list of targets was not confined to Ukrainian sites. In January 2015, CyberBerkut claimed responsibility for a cyber attack on German Government sites, demanding that Germany end its support to the Ukrainian government. On the pro-Ukraine side, the Ukrainian Cyber Troops reportedly claimed to have hacked into Russian interior ministry servers and CCTV". STINISSEN, J. A., *Legal Framework for Cyber Operations in Ukraine*, op. cit., p. 130.

445 WAXMAN pone de manifiesto esta situación, al afirmar que, "*The nature of digital information infrastructure facilitates anonymity, and adversaries can route their attacks through others' computer systems. Meanwhile, forensics are such that it may be very difficult to link a penetration or disruption of a computer or information networks to the responsible party, though forensic capabilities are generally improving, albeit unevenly across states. Moreover, even if investigation processes can trace a cyber-attack back through digital networks to its source, it may be difficult to publicize that information in a timely and convincing way, especially when states or private entities are likely to have strong incentives not to discuss the technical details of informational security breaches or reveal their own capabilities to adversaries or third parties. As a case in point, the U.S. government waited two years before disclosing that in 2008 it suffered "the most significant breach of U.S. military computers ever" when a flash drive inserted into a U.S. military laptop surreptitiously introduced malware into the Pentagon's classified and unclassified computer systems. Even then, the U.S. government disclosed few details about the extent of harm and said nothing about its knowledge of the likely perpetrators. Iran has likewise been very reticent about Stuxnet, its effects, and Iran's knowledge of the code's source*". WAXMAN, M. C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, Yale Journal of International Law, vol. 36, issue 2, 2011; pp.421-459, en particular, pp. 421 y 443-444.

Antes de entrar a abordar las cuestiones especificas relativas a la atribución, se impone una matización en el planteamiento, que ha sido expuesto a lo largo de la Primera Parte del presente trabajo. No puede abandonarse la tesis de que, en efecto, al conflicto armado que se libre por medios cibernéticos le será de aplicación, de forma plena, el DIH de los conflictos armados, como si se tratara de cualquier otro método de combate. Pero esto no impide que se tenga en cuenta que dicha aplicación implicara una serie de dificultades, de índole práctico que, ahora más que en ningún otro momento, se evidencian como determinantes. Si bien no corresponde al jurista en ningún caso resolver las cuestiones relativas a la indagación de los hechos, sino la calificación de los mismos una vez acreditados, sin embargo, en este caso, no puede obviarse que la indagación de estos hechos que aquí se estudian conllevará una dificultad que condicionará la propia calificación.

En el Capítulo correspondiente al análisis del contenido de la obligación de DIH, ya se ha hecho sucinta alusión, al hecho de que, el ataque cibernético quedará ubicado, geográficamente, en función del lugar en que radique el IP, correspondiente a su autor. No obstante, la argumentación que, en ese momento, era sencillamente expuesta, requiere aquí una ampliación, en el sentido de hacer constar la dificultad que entraña, incluso, la indagación de ese IP. Con carácter frecuente, la mera existencia de una IP se ha revelado insuficiente para poder atribuir todos los hechos ilícitos, por más que pudiera parecer la respuesta más evidente. Antes bien, las posibilidades fácticas de enmascarar dicha IP son tantas que, será necesaria una técnica procesal, realmente depurada así como, una legislación procedimental adecuada, en la mayoría de los Estados que compartan intereses, para poder indagar de modo fiable en la autoría de los ataques.

En este mismo sentido, se ha expresado la doctrina penalista al poner de manifiesto la insuficiencia de la IP como criterio de identificación del autor de un ciberdelito porque, como dice SALA, «*Creemos falsamente los Abogados que con la identificación de la IP ya está todo "solucionado" y esperamos que con la comunicación de la compañía proveedora de Internet ya esté todo "resuelto"*». Sin embargo, como la propia autora expone, en ocasiones, dicho IP se halla encubierto en una NAT que,

a su vez, impide concretar desde cuál de los diversos IP que operan a través de esa NAT, se ha cometido el ilícito en cuestión[446].

Estas especiales dificultades, que aquí se reflejan, han sido analizadas, asimismo, de forma pormenorizada por OTAN. La Organización, al respecto, afirma que la complejidad a la hora de adoptar medidas para la ocultación de la identidad en la red, varía de forma sustancial, de la misma manera que lo hace la dificultad técnica que pueda alcanzarse y la accesibilidad, por parte de los interesados a las distintas soluciones. Sin embargo, de modo esquemático, se advierten como más comunes la utilización de proxy, el uso de VPN y, por último, las redes TOR[447]. En los tres casos, el uso de la técnica impide una

446 La autora recoge las dificultades en la indagación de la autoría de determinados ciberdelitos, afirmando que, en ocasiones el abogado recibe escritos de tal índole, que reflejan la dificultad en la indagación del delito: "(…) cuál es nuestra sorpresa al encontrarnos con un texto como éste: "*En cumplimiento del requerimiento arriba referenciado, (...) se pone en su conocimiento que las IP relacionadas en su requerimiento son de las denominadas "NAT" (Network Address Translation,) a través de las cuales se conectan multitud de clientes por lo que será preciso conocer el puerto de la IP de origen para identificar a los usuarios concretos*". Pues bien, al respecto, la autora aclara que "*NAT: Es un desarrollo tecnológico que permite que una misma dirección IP pública sea utilizada simultáneamente por una multitud de direcciones IP privadas asignadas a clientes de una determinada red. Esto se hizo necesario porque IPv4 fue diseñado sólo para conectar unas cuantas universidades y redes militares, con sólo cuatro mil millones de direcciones, que se hicieron insuficientes para un despliegue comercial de Internet. NAT permite multiplicar una única dirección IPv4 pública para que la usen hasta 16,7 millones de dispositivos dentro de una misma red (usuarios/dispositivos de una empresa, de una familia, etc.). La dificultad se centra en que, los requisitos legales actuales a los operadores de Telecomunicaciones no obliga a registrar los puertos, y que los routers, tampoco conservan en memoria los datos de los puertos peticionarios y, en caso de investigación cibercriminal, será difícil conocer el ordenador solicitante*". Por último, en el mismo documento, SALA menciona la importancia de la IP en el Orden Jurisdiccional Penal y cita la Sentencia de la Sala 2ª del Tribunal Supremo el 3 de diciembre de 2012, núm. 987/2012, cuyo Fundamento de Derecho Tercero expresa: "*(…) La inferencia que vincula ser usuario de un ordenador y línea telefónica no lleva a (…) la conclusión de que ese usuario sea autor de toda utilización telemática de esa infraestructura informática*". *Siguiendo a continuación con que, al tiempo de los hechos el entorno utilizado en ese caso era Windows XP Professional edición 32 bits con antivirus gratuito y conexión módem, lo que implicaba que en internet estuvieran publicados los puertos que estaban disponibles en el PC(…) Hablamos aquí de la posibilidad de que un tercero no imputado esté cometiendo un delito utilizando una vulnerabilidad de un soporte y manteniendo el ordenador zoombie, es decir, a su libre uso y disposición en remoto y sin conocimiento del titular. Concluyendo, aún solicitando la IP, estaríamos más ante una posibilidad de suma de prueba indiciaria que si cumple los requisitos que prescribe, entre otras, la Sentencia del TC 128/2011 también podría sustentar un pronunciamiento condenatorio*". SALA ORDOÑEZ, R., *NAT, autoría en ciberdelitos*. 14 de marzo de 2016. Disponible en el sitio web: www.abogacia.es/2016/03/14/nat-autoria-en-ciberdelitos/#. Fecha consulta, mayo de 2014.

447 El artículo que publica el Centro de Excelencia de OTAN, ofrece una exposición y análisis de estos medios tecnológicos que, de forma resumida se pasa a transcribir para una mejor comprensión del presente capítulo. Proxy es definido del siguiente modo: "(…) *is a type of computer service which collects access requests from clients and forwards them to the destination on behalf of the requestors. After receiving replies, the proxy sends back the information to the requestor. It works like an intermediary service between sources and destinations. There are also different types of proxies such as reverse proxies which focus on distributing server load, accelerating TLS/SSL, or optimising content by*

identificación sencilla de atacante, aunque desde un punto de vista práctico las implicaciones son distintas. No obstante, es preciso hacer constar que, dichas técnicas se hallan al alcance, tanto de los Estados, como de los particulares. Esto quiere decir que dichos proxy, VPN o redes TOR serán utilizados, por los distintos agentes estatales o no estatales, en la comisión del hecho ilícito. Por ello, como se ha anticipado, las doctrinas que, a lo largo del presente Capítulo, se irán planteando, en cuanto a la atribución de hechos ilícitos, a agentes estatales y no estatales, deberán ser entendidas en el contexto que aquí se expone.

En estos casos, pues, al igual que sucede en la indagación de otros ataques informáticos, que, sin llegar a ser un ataque armado, resultan ilícitos, conforme al Derecho interno o internacional, resulta esencial contar con una depurada técnica forense, que ofrezca al jurista las necesarias garantías en cuanto a la acreditación de los hechos y la autoría así como, con una normativa adaptada, a estas nuevas modalidades comisivas del ilícito.

---

compressing it in order to speed up loading times. Proxies can be used both for internet filtering and bypassing such internet filtering attempts. If this channel to the proxy cannot be detected and blocked within the perimeter, they would be able to circumvent the limitations and bypass the restrictions". Por otro lado las VPN son recogidas en el mismo documneto en el siguiente sentido: "*A Virtual Private Network (VPN), which is the most common solution for network tunnelling, is a way to channel all or in some cases part of the network traffic via a different middle node. Technically, it is a private network and provides inter-connectivity to exchange information between various entities that belong to the VPN. In most cases, VPNs are used to access internal networks such as a company's intranet resources. Since VPN traffic is encrypted and can be used like a proxy, it is another way to bypass internet censorship. Confidentiality, integrity and authentication tenants of security are available in a VPN so that, even if the network traffic is sniffed, attackers would only see encrypted data and not the plain text. Integrity of communication is also provided, so that any sort of tampering would be detected and discarded from the network. Domain Name System based bypassing Basically is a translation mechanism which converts domain names to IP addresses. When it comes to filtering, DNS is another option for enforcing censorship. Since the initial step is to learn the IP address of the target service, a DNS server can be configured to block access to that service. If a specific domain name is black-listed, DNS would simply block access to that web site by not answering the DNS request. It is also possible to configure DNS to return a different IP address for a specific query, which would result ending up on a totally different web site*". Por ultimo la naturaleza y funcionamiento de las llamadas redes TOR es expuesta de la siguiente manera: "*Onion routing is a networking mechanism which not only ensures that the contents are encrypted during network transmission to the exit node, but also hides who is communicating with whom during the process. It is a general purpose infrastructure for private communications over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis between the relays of the network, although exit nodes can monitor the traffic since they transmit the network packets to their destinations. Censorship circumvention efforts mostly focus on what is observable by authorities in a network channel, with the aim of bypassing them. Encrypted channels, which are created between each relay in onion routing, are therefore very effective. Using Tor together with proxies and VPNs makes it even more resistant*". ÇALIŞKAN, E., MINÁRIK, T., OSULA, A.M., Technical and Legal Overview of the TOR Anonymity Network. NATO Cooperative Cyber Defense Centre Of Excellence. Tallin 2015; pp.3-7.

En este sentido, la doctrina ha puesto en relieve la importancia que tiene el mero hecho de compartir información y datos La colaboración entre Estados y, entre los Estados y las entidades privadas, ha de tenerse por un mecanismo de seguridad efectivo. Esta necesidad ha sido expuesta en documentos como la Cyberspace Policy Review de los Estados Unidos publicada en mayo de 2009[448]. Sin embargo, autores como LOBEL entienden que dicha intención no ha sido concretada en medidas oportunas y que la ambigüedad que de ella se desprende, se mantiene en documentos posteriores[449].

De este modo, la localizacion de la IP resulta claramente insuficiente y, como afirma PIHELGAS: "*It is not enough to just locate a source IP address (unless looking solely at active defence): the identity of the attackers must be determined, as well as the parties they were acting on behalf of must also be unmasked*".[450] En consecuencia, como el mismo autor pone de manifiesto, la necesidad de colaborar, a través de macanismos que obliguen o incentiven a los Estados a compartir datos por parte de estos y de los particulares, resulta esencial. Sin embargo, las reticencias que se encuentran al respecto pudieran frustrar dicha colaboración y, entre las razones por las que se justifica la falta de colaboración, en la medida que resultaría

448 El documento "*Cyberspace Policy Review. Assuring a Trusted and Resilient Information*", ha sido publicado por el Gobierno de los Estados Unidos en mayo de 2009. El mismo esta dicponible en el sitio web: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pd. Fecha de consulta, febrero de 2015. Asimismo, es recogido por LOBEL que, al respecto sostiene que, "*The report reiterated the necessity of building private-public partnerships to facilitate cyber incident information sharing and to coordinate efforts to "detect, prevent, and respond to significant cybersecurity incidents". "(…) while civil liberty advocates are concerned that this information sharing might invade individuals' privacy*". LOBEL, H. *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, op. cit.; p.635.

449 Así, el mismo autor entiende que:" (…) *The State Department's May 2011 International Strategy for Cyberspace reiterates the need to partner with the private sector, but does not provide clarity regarding how private-public partnerships could be implemented in compliance with the law of war*". *Ibidem*; p.636.

450 PIHELGAS y PARK, en este sentido, continuan afirmando que: "*In order to supplement the solely technical means of attribution, collaborative data exchange must ensure that when large amounts of data are brought together, data mining techniques and statistical analysis can afford us additional clues as to the author of such tools with a higher degree of certainty than technical means or independent data alone. By correlating the shared information, a more effective method for a community to detect potential risks and prevent cyber attacks at an early stage can be developed.*" PIHELGAS, M. y PARK, G. *Cyber Information Exchange. Collaboration for Attribution of Malicious Cyber Activity*. PIHELGAS, M. (Ed.), Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks. NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn, 2015; pp. 8-23., en particular, p. 8.

aceptable, se encuentran la siguientes[451]: en primer lugar, el citado autor entiende que, para ellos, es necesaria una confianza entre las partes llamadas a prestarse mutuamente dicha colaboración y esta necesaria confianza no siempre está presente. A juicio del mismo, una falta de fiabilidad en la integridad de los datos recibidos pudiera originar que el programa destinado a compartirlos está también predestinado a fracasar. Esta desconfianza, además, sufre un incremento proporcional al número de partes que configuren el programa de que se trate[452].

Sería necesaria pues, una concienciación global en materia de ciberseguridad que, además, estimulara a entes públicos y privados, a hallar los mecanismos oportunos, para conseguir tal intercambio de información. Por otra parte, el mismo autor entiende que es necesario superar el obstáculo, del daño en la reputación, para comprometerse en un programa de intercambio de información[453], pues no cabe duda de que, comprensiblemente, la trasmisión a terceros, de datos comprometidos, exige una plena confianza, en el depositario de dicha información así como, la aceptación de que las vulnerabilidades de un sistema van a ser expuestas. Esta revelación de las vulnerabilidades conllevará, indefectiblemente, una merma en la imagen pública de un Estado o corporación privada y, tambien, en ocasiones, una previsible disminución, en la confianza que pueda generar su ciberseguridad. Por lo tanto, nos encontramos ante factores que

---

451 Los mismos autores exponen que: "*the rate of data exchange is not near the level it needs to be in order to effectively stem cyber incidents, let alone to assist with attribution*". PIHELGAS, M. y PARK, G. *Cyber Information Exchange. Collaboration for Attribution of Malicious Cyber Activity*, op. cit.; p. 9.

452 Una solución, a juicio de los autores, podría ser la propuesta en los siguientes términos: "(…) *federated domains or trust partnerships can be established within a programme. This would allow for a number of communities with particular interests or relationships to share information whilst maintaining the Confidentiality and Integrity elements of the CIA triad*". PIHELGAS, M. y PARK, G. *Cyber Information Exchange. Collaboration for Attribution of Malicious Cyber Activity*,op. cit; p. 9.

453 Los autores lo explican del siguiente modo: "*Whilst there may be a long list of organisations and governments wishing to consume cyber threat information, sharing programmes in any form suffers from two kinds of parasitic users, and despite the content of these exchanges, both lurkers – those who observe but do not necessarily contribute – and leechers – those who maintain a negative ratio of downloaded or uploaded data – are common. Knowledge of an adversary's TTPs2 is advantageous … but sharing of this information may put the contributor at risk by exposing the protective or detective capabilities of the organization and result in threat shifting by the adversary.' No rational state is likely to dispose of its strategic advantages in these areas by making actionable information available to every other nation in the world through a multilateral organization. Effective trust partnerships limit the ability to contribute without naming the author but the only way this could be truly implemented is by way of an information broker who would act as a cut-out for any organisation wishing to contribute sensitive information without fear of attribution. The impact of this must be understood, as without an author, contextual understanding is more difficult and the data begins to lose an element of integrity and thus its credibility*". *Ibidem*, p. 9.

deberán asumirse, en el momento de comprometerse en el programa de intercambio de información. De hecho, pudiera ser éste el principal motivo, por el que los daños que, realmente, sufren los Estados y las empresas, al ser objeto de ciberataques, no son conocidos con detalle. En realidad, reconocer estas situaciones supondría tanto como exponer las zonas más deficientes, en seguridad, a futuros atacantes. Por último, el mismo autor expone las dificultades, de índole económica, con las que los Estados y los organismos privados pueden encontrarse, a la hora de abordar su participación en uno de estos programas[454].

Pues bien, en el ámbito específicamente español, cabe destacar que la mayoría de las reticencias, que aquí han sido expuestas y, que impiden la verdadera consecución de una conciencia de seguridad, han sido contempladas por el Instituto Nacional de Ciberseguridad (en adelante, INCIBE). La actividad de este Instituto se halla orientada a ofrecer una serie de servicios y actuaciones, entre cuyos beneficiarios, puede encontrarse tanto a entes públicos, como privados, a los que ofrecen instrumentos que permiten un desarrollo de su labor profesional con mayor seguridad. En esta labor el INCIBE se dedica, fundamentalmente, a la prestación de servicios en el ámbito de la ciberseguridad, que permitan el aprovechamiento de las TIC y eleven la confianza digital, trabajando así en la protección de la privacidad de los usuarios[455]. Asimismo, según su propia definición, el INCIBE fomenta el establecimiento de mecanismos, para la prevención y reacción a incidentes de seguridad de la información, minimizando su impacto en el caso de que se produzcan. Por otro lado, también promueve el avance de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación. Este Instituto, que se articula jurídicamente a modo de sociedad anónima[456], desarrolla, asimismo, una labor de investigación, que aborda proyectos, de forma tal que el Instituto declara tener capacidad para generar inteligencia en ciberseguridad. Por último, además de la

454 *Ibidem*, pp. 9-10.
455 Así puede leerse en su propia página web: www.incibe.es/que_es_incibe. Fecha de consulta, diciembre de 2015.
456 Respecto a la naturaleza jurídica, composición y funcionamiento, de dicho centro, consultarse el sitio web: www.incibe.es/que_es_incibe. Fecha de consulta, diciembre de 2015.

prestación de servicios y la tarea de investigación, el INCIBE se define como un Instituto participante en redes de colaboración, que facilitan la inmediatez, globalidad y efectividad, a la hora de desplegar una actuación, en el ámbito de la ciberseguridad y, en este sentido, el referido Instituto entiende imprescindible para la consecucion de todo ello, la coordinación y colaboración con otras entidades, tanto públicas como privadas, nacionales e internacionales, de todo el ámbito de la ciberseguridad. No cabe duda de que los propósitos que el citado organismo se plantea, como objetivos a conseguir, resultarían de gran utilidad en el ámbito práctico, caso de ser logrados, pues se encuentran encaminados, todos ellos a mermar las dificultades, que antes habían quedado expuestas por la doctrina foránea, en orden a conseguir la precisa colaboración en materia de seguridad.

Pues bien, en este ámbito interno en el que nos encontramos, parece que los objetivos expuestos por el INCIBE tienen un grado de consecución ciertamente satisfactorio y que, en el ámbito jurídico que nos ocupa, el Instituto es acreedor de una reputación favorable.[457].

En este punto, conviene recordar que la dificultad de atribución del hecho ilícito se constatará, sea este producido hecho ilicito por un Estado o, por un particular, pues las posibilidades de ocultar el verdadero origen, del ataque informático, estarán al alcance de ambos. Sin embargo, la presencia del Estado, en determinadas redes ocultas, debería utilizarse, precisamente, para permitir una mejor indagación de los hechos. En cualquier caso, la atribución al Estado, de los hechos ilícitos cometidos por sus órganos, no debería plantear dificultad, más allá de la indagación de la autoría. En cualquier caso, se trata de cuestiones que se abordarán en el epígrafe inmediatamente posterior.

457 Así, se considera que entre las herramientas de utilidad para el abogado que el INCIBE difunde, se pueden citar, la aplicación CONAN Mobile, útil para identificar vulnerabilidades de los terminales móviles con sistema operativo Android; el servicio antibotnet, que permite identificar si la dirección IP desde la que los terminales se conectan puede estar comprometida por formar parte de una red de bots (*botnets*) o como comúnmente se conocen, "ordenadores zombies"; el kit de concienciación, gracias al cual las organizaciones pueden, de manera práctica, tomar conciencia y adoptar medidas eficaces de protección frente ciberataques; o el CERT de Seguridad e Industria (CERTSI) desde el cual se gestionan servicios de soporte para afrontar ataques de especial gravedad. Estas herramientas son citadas por PÉREZ BES, F., *El rol del abogado en la ciberseguridad*. 14 de diciembre de 2015, doc. cit.

Por último, la dificultad de atribución del ilícito internacional, cuando éste es producido por un particular, ha llevado a la doctrina internacionalista a defender que debería rebajarse el nivel de control, exigido al Estado, en los supuestos en que los ciberataques se producen, en el desarrollo de un conflicto armado[458]. Sin perjuicio de que esta cuestión será objeto de análisis más detallado, al final del presente Capítulo, puede avanzarse ahora que, la tradicional doctrina, en relación a la atribución al Estado, del hecho ilícito cometido por un particular, requiere una adaptación a este nuevo método de combate. De otro modo, la comisión de un hecho ilícito cometido por un particular, que no pudiera atribuirse a ningún Estado, podría suponer una ventaja desmedida para el Estado que es parte en un conflicto armado. No puede ocultarse que, como se vera, las exigencias en los criterios de atribución implicaran la imposibilidad absoluta de atribución en determinados casos, pero en modo alguno puede esta consideración justificar un aminoramiento en dichas exigencias.

De nuevo, pues, nos encontramos ante una situación en la que, la novedad de este método de combate conlleva que las referencias sean escasas, pues no contamos con una normativa convencional que haya sido ya adaptada al mismo. A ello hay que añadir, la falta de práctica suficiente de los Estados que, ejercida junto con la correspondiente *opinio iuris*, constituya un Derecho Consuetudinario propio de este ámbito[459].

458 ALLAN, C.S. "*This test must lower the required degree of connection between a state and a non-state cyber attacker before a state may be responsible for the non-state cyber attacker's actions*" ALLAN, C.S. *Attribution Issues in Cyberspace*, op. cit.; p.60.

459 SCHMITT y VIHUL, defienden en este sentido que "*Absent opinio juris, it is difficult to assess whether the community views particular actions as legally mandated (or forbidden) or as simply the product of policy decisions*". A su juicio, la postura que los Estados adoptan en relación a estas cuestiones depende de la relación que los mismos hallan desarrollado con la tecnología: "*On the one hand, IT-dependent states that are most vulnerable to hostile cyber activities have an incentive to characterize hostile cyber activities as violations of international law. On the other hand, IT-dependency often goes hand-in-hand with IT-capability; states that have developed an advanced cyber infrastructure are also the most likely to possess offensive cyber capabilities*". SCHMITT, M. N. & VIHUL, L., *Proxy Wars in Cyberspace*. Fletcher Security Review vol I, issue II, Spring 2014; pp.55-73, en particular, pp. 59-60.

3. CIBERATAQUES ORIGINADOS POR EL ESTADO.

Los ataques informáticos, que constituyan un ataque armado, en el sentido argumentado en la Primera parte del presente trabajo, serán lanzados, con toda seguridad por parte de los componentes de las Fuerzas Armadas, del Estado de que se encuentre un conflicto armado, sea éste internacional o no internacional. Es decir, si bien ya se ha mencionado la diversidad de actuaciones que podrán hallarse en la red, el hecho de que internet pueda ser usado como un arma, exige que el uso de ella, como método de combate, por parte de quienes se encuentran obligados a combatir, sea examinado en primer lugar.

Se trata, por lo tanto aquí, de ver en qué situaciones el Estado es responsable de la acción u omisión de los hechos ilícitos cometidos por los miembros de esas Fuerzas Armadas, cuando éstos son los encargados de llevar a cabo las operaciones de ciberdefensa y, también, en aquéllos supuestos en que se cometan dichos ilícitos cibernenticos, por parte de militares, que no forman parte de estas Unidades especializadas.

3.1. Ciberataques lanzados por órganos estatales.

Los cibercombatientes se integrarán, con toda normalidad, en las Fuerzas Armadas de un Estado y, por lo tanto, estarán sometidos al Derecho interno de ese Estado, así como al DIH. Como consecuencia de ello, a dichos atacantes les será de aplicación el estatuto de combatiente, del mismo modo que si manejaran cualquier otro armamento o método de combate. No se pueden dejar de tener en cuenta, en este momento, las apreciaciones que han sido realizadas, a lo largo de la Primera Parte del presente trabajo, en relación a la conceptuación de los ciberataques como ataque armado y de internet como arma de doble uso. En consecuencia, a quienes empleen dicho método de combate, de forma aislada o, en conjunción con otros que pueden formar parte del desarrollo del combate, les será de aplicación las normas relativas al combate. Por lo tanto, cuando se cometa la violación de cualquiera de las obligaciones que han sido analizadas en el Capitulo precedente, el hecho ilícito, *a priori*, será atribuible al Estado parte en el conflicto.

3.1.1.- La responsabilidad del Estado derivada de la actuación de los miembros de las Fuerzas Armadas.

El Proyecto de artículos hace referencia, en este sentido, a la directa responsabilidad internacional, exigible al Estado, respecto de los hechos ilícitos cometidos por sus órganos. Así, el artículo 4 de mismo entiende que:

> "1.- Se considerará hecho del Estado según el derecho internacional el comportamiento de todo órgano del Estado, ya sea que ejerza funciones legislativas, ejecutivas, judiciales o de otra índole, cualquiera que sea su posición en la organización del Estado y tanto si pertenece al gobierno central como a una división territorial del Estado.
>
> 2.- Se entenderá que órgano incluye toda persona o entidad que tenga esa condición según el derecho interno del Estado".

Puesto que no cabe duda de que se podrá exigir la responsabilidad internacional al Estado, por las violaciones de normas de DIH que se cometan por sus órganos, resulta primordial determinar qué se entiende por Estado, ya que este, como sujeto de Derecho Internacional, podrá manifestarse de diversas formas, en el plano jurídico. En este sentido, si se pretende determinar la responsabilidad internacional del Estado por la violación de obligaciones internacionales de DIH, hay que hacer una especial mención a las Fuerzas Armadas, pues será, a través de la actuación de las mismas, como de forma mayoritaria, se constate dicha violación. No pueden dejarse al margen, tampoco, los supuestos en que, la contravención de una norma de DIH se producirá por parte de un particular o, en cualquier otra de las manifestaciones, que se analizarán en el epígrafe posterior. Sin embargo, el uso de la fuerza, monopolio del Estado, vendrá referido a las Fuerzas Armadas en combate y, por ello, el Estado será responsable de los hechos ilícitos en el cumplimiento del DIH a través de ciberataques, en forma que va a analizarse.

El DIH no es ajeno a esta cuestión y esta responsabilidad aparece reflejada en el en el PA I, que establece que el Estado sera responsable de "*todos los actos cometidos por las personas que hagan parte de su fuerza armada*[460]".

La aplicación de esta norma general, de atribución de responsabilidad en DIH, se refleja en los cuatro Convenios de Ginebracomo se puede comprobar en la Compilación de DIH consuetudinario,"*que establecen la existencia de la responsabilidad del Estado, además de la obligación de enjuiciar a las personas que cometan infracciones graves*"[461].

La responsabilidad por el hecho ilícito, como ha sido puesto de manifiesto en la Primera Parte, podrá originarse por la comisión de ese ilícito, bien a través de una conducta activa, bien omisiva. Es decir, que el hecho ilícito, del que deba responder internacionalmente el Estado, puede constituir una acción, a través de la que se viola una norma de DIH o bien, la omisión de una obligación, como la que pueda tener un Estado "*de ejercer diligencia a fin de evitar comportamientos contrarios al derecho internacional humanitario, y de enjuiciarlo y sancionarlo si ocurre*"[462] .

Es decir, que el Estado responderá, también, por omisión de los hechos ilícitos que se produzcan, cuando dicha causacion sea consecuencia de la inobservancia de su deber de cuidado. En coincidencia con lo que afirma SASSOLI, puede sostenerse que la obligación de "*hacer respetar*" el DIH presente en el artículo 1 común a los Convenios de Ginebra, "*establece una norma de la diligencia debida por lo que respecta a los agentes privados si éstos están bajo la jurisdicción de un Estado, o incluso por lo que atañe a las infracciones del derecho*

460 En ese sentido se expresa el artículo 91 del PA I, cuyo texto completo establece que "*La Parte en conflicto que violare las disposiciones de los Convenios o del presente Protocolo estará obligada a indemnizar si hubiere lugar a ello. Será responsable de todos los actos cometidos por las personas que formen parte de sus fuerzas armadas*".

461 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; pp. 599-606.

462 SASSOLI, M., *La responsabilidad del Estado por las violaciones del derecho internacional humanitario*. Revista Internacional de la Cruz Roja. Junio 2002. Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/5tecbx.htm. Fecha de consulta, junio de 2013.

internacional humanitario cometidas por Estados o por agentes no estatales extranjeros que podrían estar influidos por un Estado"[463].

Por lo tanto, nos encontramos con que existe una obligación genérica, de respetar el DIH, común a los Convenios de Ginebra, que puede ser incumplida por omisión y tambien, con el hecho de que, como se ha anticipado, existen unas normas llamadas cardinales o, principios inconculcables de DIH, que han de ser respetados, en todo momento y en todo conflicto, bajo cualquier circunstancia. A mayor abundamiento, hay que tener presnete que, ademas, el DIH contiene una serie de normas cuya violación constituye un ilícito especialmente grave, de modo tal que, su naturaleza podria considerarse constitutiva de *ius cogens*. De ser asi, como se vera en el Capitulo posterior, su violación podría ser denunciada por la Comunidad Internacional, en su conjunto y, por lo tanto, sin necesidad de que el Estado lesionado por la violacion de la obligacion, inste su reparacion. De cualquier modo, como tambien se vera dichas obligaciones impedirán ejercer una oposición persistente, en el ámbito del DIH consuetudinario.

Como acertadamente pone de manifiesto el CICR, el artículo 1, común a los Convenios de Ginebra, al imponer la obligación de respetar y hacer respetar el DIH, no contempla el modo concreto en que dicha obligación tenga que ser cumplida. En la labor destinada a delimitar las funciones integrantes del cumplimiento de esta obligación, el CIRC entiende que, las medidas que los Estados deberían adoptar, pasan por la presencia de un asesor jurídico, que preste la necesaria asistencia para el desarrollo y adaptación de la normativa interna al DIH. También contempla el adiestramiento adecuado, de los asesores específicos de las Fuerzas Armadas[464].

---

463 SASSOLI, M., *La responsabilidad del Estado por las violaciones del derecho internacional humanitario*, op. cit.

464 Ya se ha hecho referencia en Capitulos precedentes del presente trabajo a la adecuación del Código Penal español a las normas de DIH y su completa implementación, no sólo en el ámbito penal, sino también disciplinario de las Fuerzas Armadas españolas. Por otra parte, la necesidad de adiestramiento del personal militar a través del asesoramiento jurídico en materia de DIH, ha sido puesta de manifiesto por DE TOMÁS MORALES, S. y VELÁZQUEZ ORTIZ, A.P., en *La responsabilidad del mando en la conducción de operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz*, op. cit.; pp. 117-150. En el mismo sentido, PALWANKAR entiende que estas medidas, además, deberían incluir: "*teaching international humanitarian law as part of any kind of military co-operation; holding regional and international seminars with the participation of States in order*

A juicio de PALWANKAR[465], tambien hay que tener presentes las medidas recogidas en el artículo 89 del PA I que establece que "*En situaciones de violaciones graves de los Convenios o del presente Protocolo, las Altas Partes contratantes se comprometen a actuar, conjunta o separadamente, en cooperación con las Naciones Unidas y en conformidad con la Carta de las Naciones Unidas*".

La responsabilidad del Estado, por los actos cometidos por los miembros de sus Fuerzas Armadas, ha sido reconocida desde antiguo, también, por la Jurisprudencia internacional. Como se pone de relieve en la Compilación de DIH Consuetudinario, son varios los casos en que la Jurisprudencia ha vinculado, directamente, la actuación de los miembros de las Fuerzas Armadas de un Estado, con la responsabilidad del mismo. Asi, a título de ejemplo, puede citarse el asunto Distomo, en el que el Tribunal alemán, en 2003, afirmo que la responsabilidad de los Estados por actos ilícitos internacionales cometidos durante las hostilidades "*comprenden la responsabilidad por los actos de todos los miembros de las fuerzas armadas*[466]". Asimismo, se citan los paradigmáticos casos de los que entendió el TPAY, de modo que, tanto en el caso Furundzija, en 1998, como en la Sentencia de apelación, en el asunto Tadic, en 1999, el citado Tribunal Internacional declaró, sin reservas, que el Estado es responsable del comportamiento de sus Fuerzas Armadas[467].

En consecuencia, cuando en el desarrollo del combate, un miembro de las Fuerzas Armadas de una de las partes en conflicto, lleve a cabo un ciberataque que sea contrario al DIH, en la medida en que éste sea atribuido certeramente a

---

to debate the specific problems associated with respect for international humanitarian law; and helping to set up and update regional data banks (or a single international data bank) on the various aspects related to national measures and their implementation". PALWANKAR, U., *Measures available to States for fulfilling their obligation to ensure respect for international humanitarian law.* International Review of the Red Cross. Documento disponible en el sitio web: https://www.icrc.org/eng/resources/documents/article/other/57jmaw.htm. Fecha de consulta, marzo de 2013.

465 Asimismo en PALWANKAR, U. *Measures available to States for fulfilling their obligation to ensure respect for international humanitarian law*, op. cit.

466 Asunto citado en la Compliacion de DIH Consuetudinario, al tratar, en la Norma 149, de la *Responsabilidad del Estado por las violaciones cometidas por sus órganos, incluidas sus fuerzas armadas.* HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; pp. 600 y 601.

467 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; p.601.

su autor, implicara la comisión de un hecho ilícito por el Estado. Asi puede desprenderse del Comentario al artículo 4 del Proyecto, que establece que "*El principio de la unidad del Estado significa que las acciones u omisiones de todos sus órganos deben considerarse acciones u omisiones del Estado a los efectos de responsabilidad internacional*[468]". No puede dudarse de la naturaleza de órgano del Estado de las Fuerzas Armadas, por más que, como sigue afirmando el Comentario citado, no sea designada ninguna "*categoría de órganos a los efectos de la comisión de hechos internacionalmente ilícitos*[469]". Antes bien, "*todo órgano puede ser la fuente de un hecho de esa naturaleza*[470]" y, en el supuesto que aquí se analiza, será, con toda probabilidad, un miembro de las Fuerzas Armadas, quien se halle en situación de cometer este ilícito internacional, por haberle sido encomendada la tarea de conducir las hostilidades y, todavía con mayor probabilidad, en el caso de que pertenezca a alguna de las Unidades militares, especialmente creadas, para el desarrollo de las operaciones cibernéticas.

No obstante, en el desarrollo del combate podrán producirse situaciones en que la actuación de ese miembro de las Fuerzas Armadas genere determinadas dudas, en relación a la atribución de esa conducta al Estado en cuestión. Estas incertidumbres deberán ser resueltas desentrañando la naturaleza de dicha actuación y, para ello, resultará necesario acudir a los criterios de interpretación que ofrece el Comentario al Proyecto de artículos. Asi, el texto elaborado por la CDI, en primer lugar, aclara que será indiferente la motivación que lleve a esa persona, en concreto, a desarrollar la actividad ilícita. Por lo tanto, con independencia de que dicho miembro de las Fuerzas Armadas, pudiera cometer un hecho ilícito sin intención de hacerlo, dicha actuación sera atribuible al Estado. En aplicación de este criterio, serán del Estado los hechos que el militar realice por negligencia o incluso, por error. Así, podría pensarse, por ejemplo, en la deficiente ejecución de una ciberoperación, a causa de un escaso o erroneo adiestramiento, a quien hubiera de llevarla a cabo. Tampoco hay que descuidar el supuesto de que el responsable de la ciberoperacion incurra en el error humano.

468 Así se expresa en Comentario 5) al articulo 4 del Proyecto.
469 *Ibidem*.
470 *Ibidem*.

En estos supuestos, pudiera darse la ejecución de un ataque desproporcionado que, sin intención por parte del atacante, causara daños superfluos o innecesarios, contraviniendo así la norma de DIH, que ha sido tratada en la parte correspondiente del trabajo. Pues bien, en ambos casos, la atribución del hecho ilícito al Estado dependerá enteramente del hecho de que quien actúa, lo haga con carácter oficial, es decir, en uso de sus atribuciones o, bajo la apariencia de autoridad. En todos estos casos, la atribución será relativamente sencilla, en el sentido de que, la indagación de la autoría llevará al mismo lugar que la de los actos de cibercombate ilícitos, que hayan sido lanzados respetando el DIH, con independencia de si dicha autoría ha sido ocultada de algún modo. En conclusión, siempre que se den estas circunstancias, el hecho ilícito será atribuible al Estado.

Sin embargo, distinto es el supuesto, también citado en el repetido Comentario al Proyecto, de la distinción que, también, ha sido reflejada en diversas decisiones arbitrales, entre la conducta no autorizada, de un órgano del Estado y la conducta, puramente privada[471]. En estos supuestos, una vez identificado el autor de dicha operación, resultará determinante establecer si esa conducta estaba, o no, autorizada por el Estado. En el presente caso, tendría que comprobarse la existencia de una autorización previa del Mando militar o, si bien, si se trata de un hecho, que el individuo realiza de forma completamente particular. En el primer caso, como se verá más detalladamente con posterioridad, podrá exigirse responsabilidad del Estado, pues el hecho ilícito le sera atribuible. Sin embargo, en el segundo supuesto, cuando pueda probarse que la actuación se ha producido a título, estrictamente particular, el ilícito que se costea con dicha acción, no sera atribuible al Estado.

Como también se puso de manifiesto, en la Primera Parte del presente trabajo, la facilidad en el acceso a este arma, de doble uso, impone un especial cuidado, en el manejo de la misma y, también, un especial interés en el adiestramiento, a quienes se hallen directamente involucrados, en el desarrollo de las operaciones cibernéticas. Así las cosas, cabe presuponer que, en todos aquellos casos en que el ciberataque se demuestre un hecho privado del

471 Así se recoge en el Comentario 13) al artículo 4 del Proyecto.

individuo, no será exigible la responsabilidad al Estado. Sin embargo, esta apriorística afirmación es susceptible de tantas matizaciones que no puede tomarse como conclusión sino antes bien, como un punto de partida en el estudio de esta cuestión.

En esta labor, hay que retomar las consideraciones realizadas, en el epígrafe correspondiente, en relación a los supuestos y condiciones en los que se trataba de la conducta omisiva del Estado. En el ejemplo anterior, podría darse la atribucion al Estado, cuando se probara una deficiente formación en quien hubiera de manejar un arma cibernética, siempre que correspondiera al Estado, en cuestión, ofrecer dicho adiestramiento. Pero, incluso en los supuestos en que se comprobara la existencia de un error humano, podría hacerse también responsable al Estado, de la falta de supervisión, respecto de esa persona en concreto y, de su acceso a determinados equipos o sistemas. Podría darse el caso de que, determinadas personas, sin estar al mando de las operaciones ciberneticas, tuvieran acceso a determinadas capacidades que, mal utilizadas originaran u hecho ilícito. Por lo tanto, la concienciación en ciberseguridad, por la que aquí se aboga, deberá comenzar por limitar el acceso al manejo de ciertos equipos, sistemas o funciones. Aun mas, dentro de los casos de acceso permitido, deberá establecerse un filtro, que impida la realización de determinadas acciones, que pudieran suponer un mal uso de la red. El acceso, por ejemplo, a un número ilimitado de destinatarios de correo electrónico, podría suponer, en el caso de un mal uso del mismo, un colapso de la red militar, que conllevara la incomunicación de los principales Mandos militares. Si dicha circunstancia se produjera en caso de conflicto armado, podría tener consecuencias nefastas en el desarrollo del mismo, por más que no se manifestara como un hecho ilícito frente a otro Estado.

En relación con la responsabilidad que, al Estado cabe exigir por omisión, resulta oportuno traer, también, a colación el ya citado Manual de Tallin que, en su Norma número 5, contiene la siguiente previsión: "*un Estado no permitirá, a sabiendas, que se utilice la ciberinfraestructura alojada en su territorio o bajo su exclusivo control gubernamental, para la realización de actos que afecten a otros Estados de forma*

negativa o sean contrarios al Derecho". Es decir, en sentido contrario, permitir el uso de dicha ciberinfraestructura podría suponer, a juicio de los autores del Manual, la exigencia de responsabilidad por omisión. La citada Norma pretende ser establecida con un ambicioso fin, pues prohíbe el uso de la infraestructura cibernética gubernamental, con independencia del lugar en que se encuentre y, de la misma infraestructura que se encuentre en territorio nacional, con independencia de su titularidad y el control que se ejerza sobre ella. Afirma, asimismo, el referido Manual que, dicha Norma pretende hacer respetar el principio de soberanía nacional. No obstante, aunque sea esta la intención declarada, parece exigirse al Estado un control tan estricto, sobre sus redes y sobre las que están presentes, físicamente, en su territorio, que no parece que esta previsión pueda llegar a tener un sencillo cumplimiento en la práctica.

Desde un punto de vista meramente teórico, no puede dejar de compartirse la construcción aportada por los autores del Manual, basada, a su juicio en que, "*States are required under international law to take appropriate steps to protect those rights*[472]". En un intento de ejemplificar dicha afirmación, el Manual cita el caso del Estado que permite que se utilice su infraestructura cibernética, por parte de un grupo terrorista, para perpetrar un ataque contra otro Estado y el Estado que consiente tal conducta, no lleva a cabo ninguna medida razonable, aun a sabiendas de las intenciones terrorirstas. En este mismo sentido se expresan SCHMITT y VIHUL al atribuir al Estado, por omisión el ilícito que no ha sido evitado pudiendo hacerlo[473].

La dificultad práctica de llevar a cumplimiento de esta medida se pone de evidencia cuando el Grupo de expertos analiza los actos futuros, es decir, aquéllos que aun no han sido materializados, pues entienden, algunos integrantes del grupo de expertos, que "*no duty of prevention exists, particularly not*

472 SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p.33.

473 SCHMITT y VIHUL, ejemplifican la cuestión del siguiente modo: "*state would therefore be required to take down a botnet's command and control server located on its territory and used by a terrorist group to carry out a largescale distributed denial of service attack (DDoS) against another state's critical cyber infrastructure, such as its electrical grid. Failure to do so is itself a breach by the state. But whether the state is responsible for the terrorists' DDoS attack is a question of attribution*". SCHMITT, M. N. & VIHUL, L., *Proxy Wars in Cyberspace,* op. cit.; p.62.

in the cyber context given the difficulty of mounting comprehensive and effective defences against all possible threats[474]".

El segundo supuesto, que se presenta a titulo de ejemplo, es el caso de que la ciber infraestructura se encuentre, bajo exclusivo control del Gobierno, aunque no se halle en territorio nacional. Se trata de un supuesto con gran trascendencia, pues será una situación muy común, en la actividad de las Fuerzas Armadas, que permanezcan desplegadas, fuera de su territorio nacional, en el desarrollo de una Operación de Mantenimiento de la Paz (en adelante, OMP) o, de un conflicto armado internacional. En este caso, el Manual atribuye al Estado, la comisión del hecho ilícito, a través de esa infraestructura que realice un tercer Estado, en las condiciones ya citadas. Por parte de los autores del Manual, se entiende que el Estado está obligado a realizar toda actuación necesaria, para impedir ese mal uso, por parte de un tercero. Ello impone, a juicio de estos autores, incluso que el Estado tenga que obligar a una empresa privada, a tomar dichas medidas si ellos fuera preciso. Para ello, logicamente el Estado debera tener conocimiento del ilicito que se va a cometer, bien a través de los servicios de inteligencia, o bien, porque el Estado haya recibido información verosímil procedente del Estado víctima.

Pues bien, aun reconociendo la utilidad de estos supuestos que los responsables del Manual de Tallin ofrecen, tampoco pueden considerarse afirmaciones que puedan ser aplicadas en cualquier supuesto. Antes al contrario, en el primer caso debería tratarse con suma cautela la atribución al Estado, porque la información de los servicios de inteligencia debería hacer referencia a actos ya realizados o que se estén realizando y no futuros, de acuerdo con la propia teoría del grupo de expertos. Es aquí donde vuelven a recobrar importancia los programas de intercambio de información antes citados, en el contexto de una cultura de ciberseguridad.

Precisamente es en este tipo de supuestos donde el consenso en la doctrina, que no ha sido alcanzado en el Manual que se expone, se hace más necesario, porque estas situaciones parecen de probable comision, en el futuro. Conforme a

474 SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p.34.

la teoría de la responsabilidad internacional por omisión, que ha sido expuesta en la primera parte del trabajo, parece claro que el Estado debiera responder por aquellos actos, cometidos en la ciberinfraestructura de su territorio o, usando aquélla sobre la que tiene control gubernamental. Esta atribución podrá realizarse si, de un modo razonable, el Estado debió conocer dicha actuación. No puede ocultarse que existen dificultades a la hora de delimitar el nivel de diligencia debida, exigible al Estado en la materia, pero los inconvenientes señalados por el grupo de expertos, no pueden ser considerados obstáculos insalvables[475].

La atribución de los hechos ilícitos, cometidos por los miembros de las Fuerzas Armadas, se dará, únicamente, según el Proyecto, cuando éstos actúan en esa condición. Sin embargo, será difícil aplicar esta teoría de forma plena, por cuanto, igual que ocurre con otras violaciones de normas de DIH, en este caso, será una tarea complicada encontrar un ciberataque, contrario al DIH que se cometa de forma estrictamente particular. Como ya se ha apuntado, el acceso a determinadas redes, equipos o sistemas debería darse, únicamente, en los supuestos en que esa persona pertenezca a las Fuerzas Armadas del Estado y, en determinados casos, aun de forma más restrictiva, a la correspondiente Unidad militar encargada de las ciberoperaciones.

Como recuerda SASSOLI, la responsabilidad absoluta, por tales actos, también se justifica por el hecho de que, los soldados forman parte de una categoría particular de órganos del Estado, sobre la que, éste, ejerce un control más estricto, que sobre otros funcionarios. En efecto, puede compartirse la afirmación de que "*al menos en tiempo de guerra y en relación con hechos regidos por el derecho internacional humanitario, los miembros de las fuerzas armadas siempre están en servicio y nunca actúan en calidad de personas meramente privadas*" [476]. Esta

475 Así se contempla en la Norma 5 del Manual de Tallin. En el párrafo 12 de dicha Norma los autores justifican la dificultad para exigir la responsabilidad por omisión "*because of such factors as the difficulty of attribution, the challenges of correlating separate sets of events as part of a coordinated and distributed attack on one or more targets, and the ease with which deception can be mounted through cyber infrastructure*" SCHMITT, M.N., Tallin Manual, op. cit.; p.26-29.

476 SASSOLI, M., *La responsabilidad del Estado por las violaciones del derecho internacional humanitario,* op. cit.

aseveración se basa en que, "*como personas privadas, nunca habrían entrado en contacto con ciudadanos enemigos ni habrían actuado en territorio enemig*o"[477].

Sin embargo, sin negar el núcleo esencial de dicha construcción teórica, de nuevo, es necesario elaborar determinados planteamientos. En el ámbito concreto de los ciberataques, sí que podría ocurrir que un militar, a título particular, accediera a una determinada tecnología y lanzar, así, un ataque cibernético contrario al DIH. En este supuesto el militar no actuara cumpliendo una orden de su superior jerárquico sino, antes bien, al margen de la orden dada o incluso sin que se haya impartido ninguna, ejecutando, así, un acto por su propia iniciativa. Se tratara, por lo tanto, de la comisión de un acto de los denominados ultra vires, que, por su singularidad y en atención a al sistemática del Proyecto, requiere un análisis especifico.

3.1.2. La responsabilidad del Estado como consecuencia de actos no autorizados. Los llamados actos ultra vires.

La responsabilidad del Estado, por la actuación de los miembros de sus Fuerzas Armadas, como órgano suyo, se extiende, según el artículo 7 del Proyecto, a los actos que dichos miembros realicen en esa condición "(…) *aunque se exceda en su competencia o contravenga sus instrucciones*".

En el mismo sentido se expresa el DIH convencional, de modo que el PA I, afirma que, una parte en conflicto "[s] *erá responsable de todos los actos cometidos por las personas que* formen parte de sus fuerzas armadas[478]".

En el ámbito del DIH consuetudinario puede hallarse idéntica respuesta, pues el Comentario a la Norma 149 admite, en aplicación del artículo 5 del Proyecto, la responsabilidad del Estado, por actos que excedan las competencias o contravengan las instrucciones recibidas. Al respecto, la Compilación de DIH Consuetudinario afirma que, "*un Estado es responsable de todos los actos cometidos por sus órganos y otras personas o entidades facultadas para actuar en su nombre, aunque*

477 SASSOLI, M., *La responsabilidad del Estado por las violaciones del derecho internacional humanitario,* op. cit.
478 Asi puede leerse en el articulo 91 del PA I.

esos órganos o personas se excedan en sus competencias o contravengan las instrucciones[479]". Como se ha señalado, al analizar cuestiones previas, resulta de utilidad la práctica estatal en la materia pues, será esta práctica, a la que, con toda seguridad, haya que acudir en el futuro, a falta de previsión normativa expresa. En este sentido, la Compilación de DIH Consuetudinario refleja la práctica de los Estados Unidos e indica que la *opinio juris* de este Estado consiste en que un Estado no es responsable de los actos "*privados*" de sus Fuerzas Armadas. Asimismo, en el comentario que la Compilación realiza a la Norma 149 de DIH Consuetudinario, trae a colación que, el Manual del Ejército del Aire de los Estados Unidos afirma que, "*el Estado no incurre en ningún tipo de responsabilidad, por las violaciones del derecho de los conflictos armados, cometidas por particulares fuera de su área general de responsabilidad, salvo que pueda demostrarse alguna deficiencia, como un nivel escaso de supervisión o instrucción*[480]". En efecto, ha de compartirse la tesis de que, dicha falta de supervisión o instrucción, serían, en principio, suficientes, para atribuir al Estado el hecho ilicito por omisión.

Por ese motivo, hay que poner énfasis en la necesidad de que estas circunstancias nunca se produzcan. Vista la accesibilidad de los miembros de las Fuerzas Armadas a la red, así como la posibilidad de aplicar conocimientos informáticos propios, a determinadas actuaciones, convendría, precisamente, partir de la tesis opuesta. Es decir, el Estado, como dice el Proyecto, es responsable de todos los actos de sus órganos. Únicamente cuando pueda probarse de forma fehaciente que el militar actuó de forma individual, podrá exonerarse de responsabilidad al Estado. Ello requerirá haber probado, previamente, que el ciberataque provenía de un dispositivo particular y no oficial. En segundo lugar, para que esta atribución no sea posible, será también necesario probar que dicho acto no responde a una orden emitida por el Mando militar. Tampoco podrá responder a un exceso en el cumplimiento de esa orden y, por último, no debería existir un deber del Estado de conocer e impedir dicho ataque.

479 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consutudinario, op. cit.; p. 602.
480 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consutudinario, op. cit.; p. 603.

Es consecuencia, la práctica de los Estados deberá ser responsable en dicho sentido y coherente con la cultura de ciberseguridad necesaria para el cumplimiento de las normas relativas al combate, pues en otro caso, la producción de daños y violaciones de las normas de DIH, a través de la red, será más que probable.

El criterio, que ha quedado más arriba reflejado en primer lugar, hace referencia a que el dispositivo utilizado, la red o el sistema sean particulares y no oficiales. En este segundo supuesto, si se puede coincidir con los autores del Manual de Tallin que, en su Norma 7, proponen que las ciberoperaciones lanzadas u, originadas, de algún modo, en una ciber infraestructura gubernamental, no es prueba suficiente para la atribución al Estado del ataque, pero es un indicio de la implicación del Estado en la misma[481]. En efecto, esta presunción resulta coherente con la norma anteriormente propuesta, pues si se permite el uso de la red y dicho uso no se impide por el Estado, de algún modo, ese Estado asume esta actividad ajena. Parece que, aun tomando esta enunciación, como mera presunción, indiciaria de la responsabilidad, resulta útil y sería deseable que los Estados ajustaran la práctica de su comportamiento a la misma.

Por lo tanto, cuando un miembro de las Fuerzas Armadas lleve su conducta más allá de lo ordenado, en principio, deberá entenderse que el Estado, al que pertenece, es responsable de dicha conducta, como tradicionalmente ha sido considerado. Solo cuando hayan sido descartadas una serie de circunstancias, como los medios a su alcance o el deber del estado de impedir el uso de los mismo, entre otras, podrá reputarse un acto estrictamente privado y se exonerará al Estado de dicha responsabilidad.

Por otra parte, la exigencia de responsabilidad *ultra vires* podrá darse en todos casos en que ese agente del Estado se exceda de sus cometidos asignados, con independencia, por ende, de la orden recibida por dicho agente. Podrá darse la atribución al Estado, por ejemplo, en la actividad de ciberespionaje cuando, al

481 La Norma 7, que los autores proponen, literalmente, dice: "*Cyber Operations Launched from Governmental Cyber Infrastructure. The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit; p. 39.

desempeñar una actividad, como la recopilación y tratamiento de información, que no es una actividad castigada *per se*, el agente, actue más allá de las normas y de las órdenes recibidas. Sin embargo, en el supuesto de los ataques cibernéticos, habrá que ver hasta qué punto es responsable internacionalmente un Estado, cuyo personal militar, utiliza, indebidamente, recursos militares, para el lanzamiento de un ciberataque que no le ha sido no ordenado. En este supuesto, habrá que temer siempre presente que ese militar no habria tenido acceso a la red ni a la información, que permita el ataque, en otra situación que no sea la del conflicto armado. Es decir, esa especial relación jurídica y, también, de hecho, que une al militar y al Estado, ha de ponerse siempre de relieve, pues el acceso del primero al armamento y a determinadas circunstancias concurrentes en el conflicto lo situan en un plano jurídico en el que al Estado le es exigible una diligencia superior que en las situaciones cotidianas. En esos supuestos, la atribución al Estado tendrá que darse, pues, conforme a los criterios ya expuestos, tanto en el caso de una conducta activa como de una omisiva.

Sin embargo, en los casos en que el militar lanza el ciberataque, desde un dispositivo particular, no será atribuible el hecho ilícito al Estado, salvo en el caso de que el Estado no tuviera modo efectivo de ejercer ningún control sobre ese dispositivo. En ese supuesto, consecuentemente, será preciso comprobar que, realmente, ha sido el titular de ese dispositivo quien ha lanzado el ataque. Es decir, vuelve aquí a ponerse de manifiesto la necesidad de una depurada técnica, en relación a la indagación de la autoría, pues también podría ocurrir que, dicho dispositivo hubiera sido usado por la otra Parte en conflicto a modo de "*zombie*"[482], para hacer ver que, el Estado en conflicto está violando el DIH y así, responsabilizar al Estado, cuyo militar, ha sido utilizado.

En consecuencia, se hace necesario reiterar la necesidad de control que, sobre los miembros de las FAS, ha de realizarse por sus Mandos, en la medida de

482 La definición de "*zombie*", asi como otros términos igualmente relevantes en este ámbito, puede consultarse en la pagina web del INCIBE: https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes/programa-mi-ordenador-es-un-zombie. Fecha de consulta, diciembre de 2015.

sus competencias y capacidades, pues ello impedirá, en granmedida la realización d ehechos ilícitos atribuibles al Estado.

3.2. La responsabilidad del Estado que presta ayuda o asistencia.

Como pone de manifiesto el Comentario al Proyecto, la responsabilidad del Estado será exigible por su concreta actuación, pero no podrá descartarse que el hecho ilícito se deba a la colaboración de otro u otros Estados, "*por ejemplo, proporcionándole a sabiendas un elemento esencial o financiando la actividad de que se trate.*"[483]

En el ámbito de la ciberdefensa, esa situación será especialmente relevante y frecuente, pues la complejidad de las actuaciones informáticas, con frecuencia requerirá de la aportación de varios Estados, para llevar a cabo el ataque. De los casos que aquí se viene citando, es el del virus Stuxnet el que, de modo más claro, ejemplifica esta posibilidad pues, como ya ha quedado apuntado, en su momento, se especuló sobre que la autoría, de dicho virus, de debiera, al menos, a dos Estados.

Esta autoría compuesta o colaborativa, está prevista en el artículo 16 del Proyecto de artículos, que establece que:

> "El Estado que presta ayuda o asistencia a otro Estado en la comisión por este último de un hecho internacionalmente ilícito es responsable internacionalmente por prestar esa ayuda o asistencia si:
>
> a) Lo hace conociendo las circunstancias del hecho internacionalmente;
>
> b) El hecho sería internacionalmente ilícito si fuese cometido por el Estado que presta la ayuda o asistencia".

Pues bien, volviendo al ejemplo antes citado y, asumiendo que el desarrollo del virus informático, se debiera a la colaboración entre dos Estados, parece que cualquiera de esos Estados podría haber incurrido en responsabilidad, en el caso de que la introducción de ese virus hubiera implicado la violación de

483 Comentario 1) al articulo 16 del Proyecto.

una obligación internacional. A juzgar por el Comentario al Proyecto, "*no debe confundirse la ayuda o asistencia que presta un Estado con la responsabilidad del Estado que comete el hecho* [484] ". En este ámbito concreto, cuando se produzcan colaboraciones de carácter tecnológico o bien, cuando se constate la cooperación, de algún otro modo, por ejemplo, permitiendo el uso de redes o la venta de armamento cibernético, será exigible la responsabilidad del Estado que presta la ayuda o asistencia. De esta norma general, se excepcionan aquellos casos en que el ilícito se habría producido, de igual modo, sin la colaboración del Estado que presta la asistencia.

La responsabilidad que puede exigirse, en virtud de esa asistencia, requiere la concurrencia de tres elementos. En primer lugar, el órgano del Estado que presta asistencia debe conocer las circunstancias, en virtud de las que, el comportamiento del Estado, que recibe la asistencia, es internacionalmente ilícito. Es decir, se exige una complicidad en el hecho ilícito tal que, ignorando el mismo, el Estado que asiste quedará exonerado de dicha responsabilidad. No obstante, ha de cuestionarse aquí la extensión de dicho concepto, relativo al conocimiento de "*las circunstancias*". En este sentido, parece aconsejable defender una postura restrictiva, en el sentido de que, únicamente, se puede exigir un conocimiento razonable, es decir aquél al que se hubiere llegado por medios oficiales, después de una indagación suficiente.

En segundo lugar, la ayuda o asistencia se deben prestar, para facilitar la comisión de ese hecho y han de facilitarla, efectivamente. A través de este segundo elemento el Proyecto de artículos está exigiendo una cooperación efectiva, no meramente intencional o tendente al objetivo.

En consecuencia, parece lógico el tercero de los elementos, que consiste en que el hecho cometido sea tal que hubiera sido ilícito si lo hubiera cometido el propio Estado que presta la asistencia. Vista la exigencia de los tres elementos y la necesidad de concreción de la conducta del Estado asistente, parece que, en relación al primer elemento hay que decantarse también por una interpretación restrictiva y exigir que, de hecho, se tuviera un conocimiento claro de la ilicitud

484 Comentario 1) al artículo 16 del Proyecto.

del hecho. Es decir, la necesaria presencia de los tres requisitos y la redacción que, de los mismos, hace el Comentario, obligan a una interpretación restrictiva de cada uno de ellos.

Una matización interesante, realizada por el comentario al artículo 16 es que, el Estado que presta asistencia, también, puede violar la obligación de no recurrir al uso de la fuerza, cuando permita que, otro Estado use su territorio, para realizar un ataque armado contra un tercer Estado. Esta forma de asistencia ha de ponerse, inevitablemente, en relación con el supuesto antes analizado, relativo a la utilización, a sabiendas, de la ciberinfraestructura de otro Estado. En este caso, el Estado que consiente, no solo conoce el ciberataque armado sino que, además, no recurre al uso de la fuerza, para evitarlo. Pues bien, si se defiende que un ciberataque es, en ciertas condiciones, un ataque armado, favorecer el uso de las redes o de servidores del Estado para que un tercero cometa un ciberataque armado, ha de entenderse como la prestación de asistencia.

Asimismo, ha de considerarse asistencia el hecho de proporcionar material a un Estado, que utilice esa ayuda, para cometer violaciones de los derechos humanos. En este caso, el Comentario al Proyecto hace constar la insistencia de las Naciones Unidas para lograr que los Estados se abstengan "*de suministrar armas y otra asistencia militar a países que se considera que cometen graves violaciones de los derechos humanos*[485]". Llevado este supuesto, al caso que aquí se trata, podría darse, por ejemplo la situación de un Estado, que desarrollara una técnica, de última generación, gracias a la asistencia de terceros Estados y que la utilizara para violar los derechos humanos, de sus propios ciudadanos. En un supuesto como ese, podría prodcirse la violación de una obligación de DIH, en un conflicto armado no internacional. Ya se ha hecho referencia a los ataques que la emisora de radio Liberty sufrió, aparentemente, provenientes del Gobierno de Bielorrusia. La constatada imposibilidad de ejercer el derecho a la libertad de expresión, en el caso de los ataques sufridos, por la página web de esta emisora, hace, de este supuesto, un caso ejemplificador de cómo, a través del uso de ciberataques, un Estado puede ocasionar la violación de derechos humanos. Por lo tanto, en el

485 Asi puede leerse en el Comentario 9) al artículo 16 del Proyecto.

supuesto de que, ese Estado se hallara inmerso en un conflicto armado no internacional y, lanzara un ciberataque, de dicha índole, contra sus propios ciudadanos, violando sus derechos humanos y se valiera, para ello, de la tecnología proporcionada por otro Estado, nos encontraríamos ante la responsabilidad de ese otro Estado por prestar asistencia.

Por otra parte, el Estado que presta la asistencia es responsable de su propio comportamiento, al ayudar, a sabiendas, a otro a violar una obligación internacional, que existe para ambos. Sin embargo, no puede reputarse responsable, del comportamiento del Estado que recibe la asistencia. En supuestos como estos últimos, la dificultad radicará, principalmente, en distinguir hasta donde llega la colaboración, de cada uno de los Estados.

La cooperación o asistencia, contenida en el artículo 16 del Proyecto, no puede extenderse al Estado que proporciona un método de combate cuando este es lícito. Ello n impide que, como afirma SASSOLI[486], cuando el Estado que proporciona ese método, conozca que va a ser usado de forma fraudulenta, debe dejar de suministrarlo al infractor. Estos casos se darán cuando un Estado preste, voluntariamente, la asistencia o ayuda a otro Estado, en la comisión de un hecho que viole las obligaciones internacionales del último, por ejemplo, proporcionándole, a sabiendas, un elemento esencial o, financiando la actividad de que se trate[487].

De la misma manera que se prevé la responsabilidad del Estado, que suministra armas a otro Estado, que cometa violaciones de derechos humanos, también, debería evitarse el suministro de armas a los Estados que cometan violaciones de DIH. En este sentido, SASSOLI, sostiene que, el Estado que presta ayuda debe "*negarse a realizar más transferencias de esas armas, aunque éstas puedan también emplearse de manera lícita*". Parece un razonamiento perfectamente asumible en el contexto que aquí interesa pues, determinados equipos, sistemas o desarrollo tecnológico podrán ser susceptibles tanto de un uso lícito como ilícito, en función de su naturaleza dual, antes expuesta. En estas circunstancias, será

486 SASSOLI, M., *La responsabilidad del Estado por las violaciones del derecho internacional humanitario*, op. cit.
487 Comentario 1) al articulo 16 del Proyecto.

determinante que, una vez comprobada la utilización que, de ellas se hace, el Estado, que presta asistencia se niegue a seguir haciéndolo, con el fin de evitar, asimismo, "*la comisión de futuras violaciones*"[488].

En la evitación de estas conductas, vuelve a ponerse de manifiesto la utilidad de los mecanismos de colaboración, destinados a compartir información, entre los entes públicos y privados, que ya han sido repetidamente mencionados. En este caso, hay que hacer mención expresa de los procesos de control de armamento, a través de los que, los Estados, se comprometen a ejercer una especial vigilancia, sobre la circulación comercial de determinadas armas o sistemas. De entre todos ellos, por la relevancia que para el ámbito de la ciberdefensa tiene, hay que mencionar el llamado Arreglo Wasenaar. Este acuerdo presenta la forma de un foro de no proliferación, del que España forma parte y tiene por objeto, de forma principal, promover la transparencia y responsabilidad de los Estados en la transferencia de armas convencionales y bienes y tecnología de doble uso[489].

El citado Arreglo no tiene naturaleza jurídica de Tratado Internacional, ni la personalidad jurídica de una Organización internacional, pero como resultado del compromiso asumido por España, en relación a los fines perseguidos por el

488 SASSOLI, M., *La responsabilidad del Estado por las violaciones del derecho internacional humanitario*, op. cit.

489 En virtud de la Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso., el arreglo de Wasenaar es un foro internacional de no proliferación, que elabora las listas de material militar y de productos y tecnologías de doble uso para ser sometidos a control de la exportación, que incluyen vectores de armas de destrucción masiva, productos y tecnologías nucleares, químicos y biológicos, así como los relativos a armas convencionales. Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso. BOE núm. 312, de 29 de diciembre de 2007. Por otra parte, el foro se constituye: "*in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists. Participating States control all items set forth in the List of Dual-Use Goods and Technologies and Munitions List, with the objective of preventing unauthorized transfers or re-transfers of those items. In fulfilling the purposes of the Arrangement as described above, Participating States have, inter alia, agreed to a number of guidelines, elements and procedures as a basis for decision-making through the application of their own national legislation and policies. The decision to transfer or deny the transfer of any item is the sole responsibility of each Participating State. All measures with respect to the Arrangement are taken in accordance with national legislation and policies and are implemented on the basis of national discretion*", según puede consultarse en la web relativa al foro: www.wassenaar.org.

mismo, se promulgó la Ley 53/2007 de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso y el Real Decreto 2061/2008, de 12 de diciembre, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso, de desarrollo de la misma. En lo que aquí concierne, es de resaltar que, los componentes informáticos se encuentran entre los que recoge el listado, que es periódicamente actualizado por el Arreglo. Esta presencia, en dicho listado implica que su comercialización requiere la previa autorización [490].

En relación a dichos componentes y, las dificultades que para su comercialización se han establecido, cabe mencionar el ejemplo del software de intrusión, definido por el listado como un

> "Software especialmente diseñado o modificado para evitar la detección por "herramientas de monitorización", o para vencer las "contramedidas protectoras" de un ordenador o un dispositivo con capacidad de interconexión en red, y que realice una de las siguientes funciones:
>
> a) La extracción de datos o información, de un ordenador o dispositivo con capacidad de interconexión en red, o la modificación del sistema o de datos de usuario; o
>
> b) La modificación del flujo de ejecución estándar de un programa o proceso con objeto de permitir la ejecución de instrucciones proporcionadas desde el exterior"[491].

490 La lista de los bienes y tecnología de doble uso y municiones data de abril de 2016 y puede consultarse en la siguiente página web: List of Dual-Use Goods and Technologies and Munitions List as at Apr. 2016. www.wassenaar.org/munitions-list-and-list-of-dual-use-goods-and-technologies/uploads/ 2016/04/ WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf. Los componentes informáticos se encuentran recogidos en las páginas 71 a 75 del citado documento. Fecha de consulta, junio de 2016.

491 RAMIREZ MORAN aclara que a esta definición le siguen dos notas que delimitan con más detalle el alcance de la definición, que excluyen e incluyen respectivamente sistemas en esta definición: «1. "Software de intrusión" no incluye ninguno de los siguientes: a Hipervisores, depuradores o herramientas de Ingeniería inversa de Software (SRE); b. "Software" de Gestión Digital de Derechos (DRM); o c. "Software" diseñado para ser instalado por los fabricantes, administradores o usuarios con propósito de seguimiento de activos o recuperación. 2. Dispositivos con capacidad de interconexión en red incluye dispositivos móviles y contadores inteligentes.» Asimismo, la definición se complementa con dos notas técnicas adicionales que especifican el significado de los dos elementos entrecomillados de la definición: «1. '*Herramientas de monitorización*': *dispositivos "software" o hardware, que monitorizan el comportamiento del sistema o los procesos ejecutándose en un dispositivo. Esto incluye productos antivirus (AV), productos de seguridad de Productos de Seguridad Personal (PSP), Sistemas de Detección de Intrusos (IDS por sus siglas en inglés), Sistemas de Prevención de Intrusión (IPS por sus siglas en inglés) o firewalls. 2.* '*Contramedidas protectoras*': *técnicas diseñadas para asegurar la ejecución segura de código, como Prevención de Ejecución de Datos (DEP por sus siglas en inglés), Aleatorización de la Distribución del Espacio de Direcciones*

De conformidad con todo lo anterior, puede concluirse que la ayuda o asistencia de un Estado a otro, para la comisión de un ilícito internacional, podrá probarse atendiendo a diversos elementos. Así, los criterios de interpretación, contenidos en el Comentario al Proyecto de artículos, resultarán de utilidad pero, vista la novedad del método de combate, nuevamente, se hace necesario acudir a otros instrumentos que, realmente, acrediten si a través del intercambio de información, el Estado que recibe la ayuda está infringiendo las normas de DIH en caso de estar en conflicto. Tambien podríamos encontrarnos, ante un Estado que recibe ayuda técnica, cuyo suministro se encuentra limitado, por alguno de los sistemas de control de armamentos a los que la Comunidad Internacional se ha comprometido[492].

En consecuencia, la trasferencia de un elemento no autorizado, por el citado Arreglo, no constituiría *per se*, la violación de una norma de DIH pero sí, un elemento de juicio, a la hora de calificar la conducta el Estado, que presta dicha trasferencia y su posible responsabilidad internacional, a la luz del artículo 16 del Proyecto.

Por último, puede entenderse que la obligación de no prestar asistencia no se limita, exclusivamente, al cumplimiento de lo dispuesto en el citado Proyecto, sino que, nuevamente hay que recordar que existe la repetida "*obligación especial que tienen los terceros Estados, (…) de "hacer respetar" las normas del derecho internacional humanitario por todos los demás Estados*". De este modo, si un Estado

---

(ASLR por sus siglas en inglés) o cajones de arena (sandboxing) ». RAMIREZ MORAN, D., *La ciberseguridad en el contexto del Arreglo de Wassenaar*. Documento de análisis 16/2012, de 9 de marzo de 2016. Instituto Español de Estudios Estratégicos; pp. 3-4. Documento disponible en el sitio web: Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_analisis/2016/DIEEEA162016_Ciberseguridad_Wassenaar_DRM.pdf. Fecha de consulta, junio de 2016.

492 La Ley 53/2007, recoge en su exposición de Motivos el objetivo de España de impulsar un Tratado Internacional sobre el Comercio de Armas y el apoyo decidido, en Naciones Unidas de la propuesta para elaborar dicho Tratado. Por tal motivo, explica la Ley, se ha decidido adecuar la legislación sobre comercio exterior de material de defensa y de productos y tecnologías de doble uso, a través de dicha norma. Además del Arreglo que aquí ha sido citado, la Ley responde a los compromisos adquiridos por España en el marco de el Régimen de Control de Tecnología de Misiles, el Grupo de Suministradores Nucleares, el Comité Zangger y el Grupo Australia, entre un gran número que es citado en dicha exposición de Motivos. Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso. BOE núm. 312, de 29 de diciembre de 2007.

prestara asistencia en el sentido que aquí ha sido expuesto, podría concluirse que "*no está ciertamente cumpliendo esta obligación específica*"[493].

4. CIBERATAQUES LANZADOS POR AGENTES NO ESTATALES.

La disponibilidad de armas informáticas, por parte de los Estados, con toda probabilidad será equiparable, en el fututo, a la disponibilidad de armas cinéticas, con la diferencia de que, algunos autores auguran un mayor crecimiento, en la importancia de la posesión de armas virtuales[494]. Pues bien, los factores que facilitan la adquisición y uso, de este tipo de armamento, motivan la preocupación por el uso que, de dichas armas, realicen los agentes no estatales. En efecto, el bajo coste económico que suponen, la fácil evitación de las bajas en combate y la posibilidad de eludir, asimismo, la identidad del autor, hasta el punto de impedir la atribución de la conducta, forman un conjunto de circunstancias, que resultarán, en igual medida, propiciadoras, de la participación de agentes no estatales en el conflicto. PADMANABHAN, al respecto apunta la posibilidad de que los Estados se hagan valer de particulares, para lanzar los ciberataques de cuya comisión, posteriormente, quieran eludir su responsabilidad[495]. Mientras que para SHACKELFORD, la dificultad de prueba en la actuación de los agentes no estatales resulta el elemento determinante, a la hora de exigir responsabilidad internacional al Estado[496] .

Esta participación de los agentes no estatales, por otra parte, tendrá cabida desde el momento en que nos encontramos ante un posible campo de batalla, accesible para todos. Es decir, como RATTRAY y HEALEY afirman, el

493 SASSOLI, M.,. *La responsabilidad del Estado por las violaciones del derecho internacional humanitario*, op. cit.

494 BRENNER y CLARKE entienden que el desarrollo de la ciberguerra se deberá en el futuro a tres factores: el bajo coste económico, el limitado número de bajas humanas que ello supone y la posibilidad de eludir la fuente de los ataques y, por lo tanto, la responsabilidad por los mismos. BRENNER, S. W. with CLARKE, L. L. *Civilians in Cyberwarfare: Conscripts*. Vanderbilt Journal of Transnational Law, vol. 43; pp. 1011-1076, en particular, p.1013-1014.

495 Así lo pone de manifietso el autor al afirmar que: "*If the State is using such a group to launch cyber operations to avoid State responsibility, then it may be very difficult to locate evidence to establish that the group is, in fact, acting under the "effective control" of the State*". PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*. US Naval War College. International Law Studies, vol. 89, 2013; pp. 288-307, en particular, p. 295.

496 SHACKELFORD, S. J., *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, op. cit.; p. 198.

ciberespacio podrá ser "*owned and operated by non-state commercial actors with their own capital and for their own reasons*"[497], de forma que ya no nos encontramos ante un lugar físico, del que se pueda desalojar, a quienes no consideremos combatientes. Antes bien, habrá que prever la posibilidad de que estos agentes intervengan, de un modo u otro y, en ese caso, en consecuencia, es ineludible considerar el régimen jurídico, que les sea de aplicación.

Esta imposibilidad de separar redes civiles y militares constituye una de las características del medio virtual, que condiciona múltiples respuestas jurídicas. Si bien esta circunstancia ya ha sido abordada, al estudiar la necesidad de distinguir entre objetivos civiles y militares, cuando se hablaba del contenido de la obligación internacional, no huelga aquí realizar una nueva mención, que ponga de relieve las consecuencias, que ello va a tener, en las cuestiones relativas a la atribución del hecho ilícito. El ciberespacio, no es un lugar físico, sino "*una experiencia interactiva virtual*[498]" por lo tanto, accesible para todos, sin que sea susceptible de una separación física.

La interconectividad entre las redes civiles y militares es una circunstancia presente en todos los Estados desarrollados, y su uso civil o militar no esta diferenciado, como se verá posteriormente con más detalle.

Pues bien, todo ello habrá de ser tenido en cuenta, cuando se aborde la cuestión de los agentes participantes en el campo de batalla virtual. La realización de operaciones informáticas, por parte de agentes estatales, en el sentido expuesto en el epígrafe previo, ha de servir de base jurídica para el análisis que aquí se emprende. No puede obviarse que los Estados son los sujetos de Derecho Internacional y, por lo tanto, los responsables de los hechos ilícitos, que éstos mismos produzcan, así como de los cometidos en su nombre.

La participación de agentes no estatales en el conflicto bélico, pues, deberá estudiarse desde una perspectiva que permita resolver en qué momento o medida el Estado es responsable de las actuaciones de los particulares, aun cuando dicha actuación haya mutado su modo de manifestarse. Como se viene

497 RATTRAY, G. J. and HEALEY, J. *Non-State Actors and Cyber Conflict.*op. cit; p. 67.
498 Así se ha definido por BRENNER y CLARKE. *Civilians in Cyberwarfare: Conscripts*, op. cit.; p.1027.

haciendo, a lo largo del presente trabajo, se trata de reformular los conceptos que, hasta ahora, se venían manejando, a la hora de atribuir, al Estado, la comisión de un hecho ilícito.

Como se verá, la participación de agentes no estatales, utilizando elementos del ámbito cibernético, simultáneamente al desarrollo de un conflicto armado, presenta una serie de caracteres que hacen que, dicha situación difiera, sustancialmente, de la que se encuentra regulada por el Proyecto de artículos, en relación con la participación de agentes no estatales. Asimismo, la participación de civiles en el combate, prevista y regulada por el DIH convencional y consuetudinario, requerirá, igualmente, una nueva consideración que permita, de nuevo, ofrecer una respuesta jurídica a situaciones novedosas. Esta labor deberá realizarse a partir de la aplicación de unas normas que, en modo alguno, pudieron prever dichas situaciones pero que, no por ello, pueden quedar al margen de la legalidad internacional.

De los supuestos que el DIH prevé, en relación con la participación de personal civil, en el conflicto armado internacional y no internacional y, que ya han sido enumerados, son dos los que, en el ámbito de los ataques armados cibernéticos, pueden dar lugar a mayor controversia. Con toda probabilidad, además serán los que se presenten, en los futuros conflictos, con más frecuencia. Son los casos de la participación de personal al servicio de empresas y de los activistas cibernéticos que entran en conflicto de manera voluntaria. En el primero de los casos, aun podrá distinguirse entre aquéllas corporaciones, de naturaleza privada, que prestan servicios a las Fuerzas Armadas, a través de un contrato y, aquéllas otras, que prestan un servicio, esencial para la sociedad y que, por lo tanto, están incluidas en el sector llamado de las infraestructuras críticas.

Actualmente, la actuación que, durante un conflicto armado, puede ofrecer una empresa privada cobra una nueva dimensión pues, entre las funciones que pueden estar llamadas a realizar, por cuenta del Estado ya no se encuentran, únicamente, las de defensa, sino que habrá que incluir también la de servicios de telecomunicaciones. En efecto, históricamente, se ha atendido al régimen jurídico, aplicable a las empresas que participan en un conflicto armado,

al objeto de dar respuesta a todas aquéllas, que realzaban funciones, tradicionalmente, atribuidas al Estado. Sin embargo, en la actualidad los servicios que las Fuerzas Armadas reciben de forma externalizada son de muy diversa índole.

Ello tendrá una evidente repercusión, en el tema que aquí se analiza, pues como se viene apuntando a lo largo del presente Capítulo, la atribución correcta del hecho ilícito requerirá una adecuada técnica. En esta tarea será necesario tener presente una nueva visión en relación al papel que, los distintos agentes, estatales y no estatales, juegan en el conflicto armado. En este sentido, tanto en los supuestos de individuos que participan a título particular, como en el de las entidades comerciales, será preciso revisar la normativa internacional y las tesis de la doctrina internacionalista, desde la óptica que ofrece el elemento cibernético.

Como punto de partida, para la realización de la labor apuntada, es preciso comenzar por atender al contenido del artículo 5 del Proyecto de artículos que aborda, en cierta medida, esta la cuestión. Al respecto, establece que:

> "Se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o entidad que no sea órgano del Estado según el artículo 4, pero esté facultada por el derecho de ese Estado para ejercer atribuciones del poder público, siempre que, en el caso de que se trate, la persona o entidad actúe en esa capacidad"[499].

La previsión contenida en este artículo 5 no hace referencia expresa, a las empresas a las que, el Estado, a través de un contrato, asigna funciones propias del mismo, pero constituye una referencia en el análisis de estas funciones. Tradicionalmente, la labor que han desempeñado las empresas privadas ha estado relacionada, con el ejercicio de facultades de seguridad y defensa y, así,

499 SASSÒLI M., BOUVIER A. A., QUINTIN A. How does law protect in war? Cases, Documents and Teaching Materials on Contemporary practice in International Humanitarian Law. Part I, Volume II. Outline of International Humanitarian Law. International Committee of the Red Cross, Case number 53; p 2.

han sido tratadas por sistemas jurídicos foráneos, por más que, en nuestro país el ejercicio de dichas funciones se haya externalizado con menos frecuencia[500].

En consecuencia, en el ámbito que ahora se estudia es necesario tener presente en qué medida las entidades privadas se hallan vinculadas con el Estado en la realización de determinadas actividades que pudieran originar un hecho ilícito, pues el uso de la red para fines militares, dependerá, en gran medida de la prestación de un servicio que ofrezca una entidad mercantil[501].

La interconectividad de redes y la prestación de servicios a las Fuerzas Armadas, por parte de empresas privadas, resulta un elemento común a los países desarrollados y con los que compartimos intereses militares. En el caso, por ejemplo de los Estados Unidos, se calcula que "*un 95% de las comunicaciones del departamento de Defensa van a través del Public Switched network y una cantidad significativa de operacional y mantenimiento de segmentos redes propiedad de los militares está llevada actualmente por civiles con base en un contrato* y que dicha interconectividad es provista "*sin distinción entre usos civiles y militares*[502]"".

Se explica, de este modo, la imposibilidad real de separar el soporte, que ampara los usos de una y otra índole, así como, la gran diferencia con la posibilidad de segregación que sí existe en el mundo físico, aplicable a otros métodos de combate y que permite el cumplimiento de la obligación de distinguir de un modo más sencillo. Es decir, en el mundo físico, la separación entre el Teatro de Operaciones y las zonas de vida civil puede realizarse, de forma más evidente, aunque no sin complicaciones. No se trata tanto de una separación geográfica[503], sino de una cuestión conceptual. No puede olvidarse

500 Al respecto, resulta de interés el trabajo realizado por LABORIE IGLESIAS, en relación a las empresas militares y de seguridad privadas, su evolución, regulación en otros ordenamientos y modelos en torno a esta figura. LABORIE IGLESIAS, M. La privatización de la seguridad. Las empresas militares y de seguridad privadas en el entorno estratégico actual. Instituto español de Estudios Estratégicos. Ministerio de Defensa. 2013.

501Así se concluye de la lectura del documento *Nodo iNET: La comunicación permite a las Fuerzas Armadas mantenerse listas para actuar*, elaborado por la empresa de telecomunicaciones BT, que puede encontrarse en el siguiente sitio web: www.bt.es/img/gestor/ministerio_defensa_red_internet_seguridad_IT.pdf. Fecha de consulta, mayo de 2016.

502 BRENNER, S. W. with CLARKE, L. L. *Civilians in Cyberwarfare: Conscripts*, op. cit.; pp. 1034-1037.

503 Esta separación geográfica es sostenida por BRENNER y CLARCKE. *Ibidem*, pp. 1034-1037.

que el DIH parte de un concepto del conflicto armado, eminentemente desarrollado por los Estados sobre el terreno, en el que, por la propia casuística de la época en que fue desarrollado, la distinción entre el objetivo militar y el civil, podía realizarse de manera que fuera comprobable físicamente. No obstante, de lo anterior no puede extraerse la conclusión de que esa separación ha de ser geográfica. Antes bien, la obligación de distinción, en el modo en que está recogida por el DIH convencional y consuetudinario, permite ser exigida, en cualquier campo en el que se desarrolle el combate. Se trata de una parte del contenido de la obligación de DIH que sigue teniendo, como se adelantaba en la Primera Parte del presente trabajo, plena vigencia y que, en modo alguno, puede obviarse, por el hecho de que las acciones de guerra se libren en un entorno virtual[504].

Por otra parte, la experiencia reciente demuestra que son varios los conflictos, de carácter internacional, en los que se ha constatado la participación de ciudadanos particulares a título individual, con cierta organización, aunque sin ningún vínculo demostrable, con ninguna de las dos partes en el conflicto. Estas situaciones distan mucho de las recogidas en el DIH convencional y consuetudinario. La Norma 149 de la Compilación de DIH, antes transcrita, prevé la responsabilidad internacional del Estado, por la comisión de hechos ilícitos en una serie de supuestos que, únicamente, a través de una nueva interpretación, podrá dar respuesta a las nuevas modalidades comisivas.

En esta reinterpretación de las normas de DIH será, de nuevo, imprescindible acudir a los criterios sentados por la Jurisprudencia internacional, para determinar, en qué casos, los cibervoluntarios, que se involucran en un

504 En este sentido BRENNER y CLARKE defienden que "*The interconnectedness of civilian and military networks means that "virtually all computer networks" can be legitimate military targets in cyberwar. This nterconnectedness will make it difficult – if not impossible – to maintain the combatant–noncombatant distinction in cyberspace. This type of civilian involvement erodes the distinction between combatants and noncombatants because civilians defending "their" networks are in a position analogous to that of soldiers defending a fort or territory to which their country lays claim*". *Ibidem*, p.1036-1037.

conflicto armado, pueden entenderse agentes participantes, por cuenta del Estado o bien, individuos de cuya conducta el Estado no tiene por qué responder.

El DIH convencional define al personal civil de modo excluyente, al establecer que son civiles, todos aquéllos que no tienen la condición militar y, por lo tanto, lo son aquéllos que no pertenecen a las Fuerzas Armadas y aquéllos que no forman parte de una *levée en masse*.

Pues bien, en relación al primer grupo, los participantes en el desarrollo del combate, ya han sido analizados en el epígrafe anterior y están constituidos por las fuerzas, grupos y unidades armados y organizados. Por otra parte, el levantamiento en masa o *levée en masse,* se da cuando la población de un territorio, no ocupado, al acercarse el enemigo, toma espontáneamente las armas, para combatir. Así pues, se trata de un personal que difiere del colectivo anterior, pues su constitución como grupo se realiza modo espontáneo y, por la propia voluntad de sus miembros, pero tiene en común con las Fuerzas Armadas, el hecho de llevar las armas a la vista y respetar las leyes y costumbres de la guerra.[505]

La principal consecuencia, entre la detentación de la condición civil o militar, en el desarrollo de un conflicto armado, viene establecida por el artículo 3, común a los Convenios de Ginebra, que establece que las Partes en conflicto deberán otorgar protección a las "*personas que no participen directamente en las hostilidades, incluidos los miembros de las FAS que hayan depuesto las armas y las personas puestas fuera de combate*". Por lo tanto, resulta imprescindible determinar, que condición jurídica es atribuida a cada uno de los distintos participantes en el combate.

4.1. Atribución al Estado del hecho ilícito cometido por empresas privadas.

En efecto, la complejidad que revisten las operaciones informáticas, en muchas ocasiones, requerirá de la contribución de personal civil, que desarrolle las herramientas informáticas e, incluso, en algunos casos, las propias

505 MELZER,N., S., Interpretive Guidance on the notion of direct participation in hostilities. International Committee of The Red Cros. Ginebra, 2009 ;p. 25.

operaciones[506]. Esta situación es relativamente previsible, para los Estados que no cuenten con expertos en ciberdefensa, entre sus Fuerzas Armadas, pero también para todos aquéllos que entiendan más beneficiosa la externalización de determinadas actividades, como el diseño del armamento informático.

De este modo, se impone la necesidad de calificar la condición jurídica de este tipo de participantes, así como la de definir el régimen jurídico, aplicable a este personal perteneciente a las empresas privadas. Se trata de establecer una premisa que permita, determinar, en un estadio ulterior, la eventual atribución al Estado de la conducta desarrollada por dicho personal.

Se trata, en este ámbito, de desentrañar si nos encontramos ante personal civil, con todas las consecuencias jurídicas que ello entraña y, que se verán más delante, de forma detallada o, por el contrario, asistimos a la participación en el conflicto, por parte de determinados agentes, que actúan por cuenta de un Estado.

En este punto es necesario acudir, como primer documento de referencia a la Guía para interpretar la noción de participación directa en hostilidades redactada por el CICR (en adelante, la Guía) que, al respecto, señala que "*para determinar si los contratistas privados y los empleados de una parte en un conflicto armado, son civiles, en el sentido del DIH y si participan directamente en las hostilidades, se utilizarán los mismos criterios que se aplican a cualquier otra persona civil*[507]".

Así pues, hay que partir de la base de que, tanto los contratistas, como los empleados civiles no están incorporados, en su mayoría, a las FAS estatales y, por tal motivo, en la mayoría de las ocasiones asumen funciones que, claramente, no implican una participación directa en las hostilidades. En consecuencia, estas personas tienen la consideración de personas civiles. Sin embargo, la citada Guía admite "*su proximidad a las FAS y a otros objetivos militares*" y expresa su preocupación por el hecho de que dicha circunstancia pueda "*exponerlos a más que*

506 Así lo prevé WATTS, S., quien además expone que "*civilian designers and contractors are likely to participate in a much more direct and ongoing fashion to CNA operations than conventional weapons designers*". WATTS, S., *Combatant Status and Computer Network Attack*. Virginia Journal of International Law, vol. 50, issue 2. 2010; pp. 392-447, en particular, pp. 410-411.

507 MELZER,N., S., Interpretive Guidance on the notion of direct participation in hostilities, op.cit.; p. 37.

a otras personas civiles a los peligros procedentes de las operaciones militares, como el riesgo de morir o sufrir heridas"[508].

4.1.1. El papel de las empresas tecnológicas en el conflicto.

Como ya se ha anticipado, en el contexto en el que en la actualidad se desarrollan los conflictos armados, las privatizaciones y las desregulaciones, en el ámbito de la defensa y de la seguridad se han convertido en una práctica frecuente. Bien es cierto que dichas funciones son de un contenido muy concreto y que, difícilmente, serán equiparables a las que aquí pretenden mostrarse. Sin embargo, con SASSOLI puede compartirse la necesidad de traer a colación la aplicación del artículo 5 del Proyecto, arriba transcrito, cuando afirma que un Estado es responsable de una persona o entidad privada que esté "*facultada por el derecho de ese Estado para ejercer atribuciones del poder público*". También en este caso la CDI pone como ejemplo el de las empresas de seguridad privadas que los Estados contratan y a las que encargan la vigilancia de las prisiones o "*las empresas en las que las compañías aéreas han delegado algunos poderes en relación con el control de la inmigración*"[509].

En el mismo sentido se expresa la Compilación de DIH consuetudinario, al entender que "*los Estados son también responsables de los actos cometidos por personas o entidades autorizadas, en virtud de su legislación interna, a ejercer prerrogativas de su autoridad gubernativa*". Pues bien, la propia Complicación justifica dicha aseveración en el reconocimiento del hecho de que "*los Estados recurren a entidades paraestatales para el desempeño de determinadas actividades*[510]". Puede extraerse aquí la conclusión de que, una vez acreditada la existencia de esta circunstancia, tanto el Derecho convencional como consuetudinario, a través de la práctica estatal, pretendieron ofrecer una respuesta a esta práctica novedosa, que impidiera la elusión de responsabilidad de los Estados, en los supuestos en que la actuación

508 *Ibidem*; p. 38.
509 SASSOLI, M., *La responsabilidad del Estado por las violaciones del derecho internacional humanitario*, op.cit.
510 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit. ;p. 602.

era atribuible a órganos, sustitutos de los estatales. De este modo, la citada Compilación afirma la existencia de responsabilidad de los Estados en relación con los "*actos de sociedades privadas o particulares empleadas por las fuerzas armadas para realizar tareas que normalmente incumben al ejército*[511]" y, en esa situación, la Compilación entiende comprendidos tanto a los mercenarios como a las empresas militares privadas[512].

Estas empresas privadas de defensa han sufrido múltiples intentos de definición y descripción, como pon de manifiesto PERCY [513]pero, en cualquier caso, la regulación, hasta ahora disponible, en relación a los hechos ilícitos, cometidos a través de los empleados de empresas privadas, deberá servir como base para determinar, cuál es el régimen jurídico de los empleados y corporaciones, que van a realizar otro tipo de actividades, en el desarrollo del conflicto armado.

Es evidente que, al margen de las entidades mercantiles que aquí se han citado, existen hoy en día una serie de compañías que, ineludiblemente, van a jugar un papel trascendental en la provisión de servicios informáticos. En consecuencia, como contratistas del Estado para las Fuerzas Armadas, deberán someterse, cuando presten servicios en un conflicto armado, a un régimen jurídico, que conviene clarificar. En el ámbito que aquí se estudia, es obvio que el personal civil, perteneciente a una empresa que preste servicios de informática, puede estar presente en el combate[514].

---

511 *Ibidem,* p. 602.

512 *Ibidem*, pp. 599-606.

513 El autor entiende que estos intentos, más bien, reflejan los retos particulares de una naturaleza particular y que dichas actuaciones están formadas por un amplio rango de actividades. Así, el autor explica: "*Many companies specialize in landmine clearance, which is relatively uncontroversial, but also offer close protection, which requires arms. The Blackwater employees that opened fired in a Baghdad market in September 2007 were engaged in close protection. The company Aegis provides both risk analysis services (as do many insurance companies) and security services in combat zones*". PERCY, S. *Regulating the private security industry: a story of regulating the last war.* International Review of the Red Cross, vol. 94, no. 887. Autumn 2012; pp.941-960, en particular, p. 942.

514 Para RODRIGUEZ-VILLASANTE, "*Los empleados civiles de empresas que suministran sistemas de armas y colaboran en su mantenimiento a menudo ocupan posiciones vitales para el combate, sirviendo como ejemplo el personal civil experto en informática del que en ocasiones depende la verificación de la naturaleza militar de un objetivo potencial*". RODRÍGUEZ-VILLASANTE Y PRIETO, J. L., *La pérdida de la inmunidad de las personas civiles por su participación directa en las hostilidades.* Cuadernos de Estrategia, núm. 172. Instituto Español de Estudios Estratégicos; pp. 167-208, en particular, p. 190.

Pues bien, con carácter general, se parte de la base del sometimiento del personal de las empresas privadas, al DIH. Esta afirmación, ha sido realizada, tradicionalmente, en relación al personal que forma parte de empresas de seguridad porque, en el desarrollo del combate, ejerce funciones muy similares, a las que son ejecutadas por las Fuerzas Armadas.

En el caso de las empresas relacionadas con la prestación de servicios de internet, este sometimiento, debería ser el mismo, pues el CICR siempre ha manifestado un especial interés en el cumplimiento del DIH, no sólo por parte de los que están obligados a hacerlo respetar el DIH, sino, también, por estas empresas militares y de seguridad privadas y su personal[515]. En opinión del CIRC es responsabilidad del Estado, proveer a dicha entidades de unas normas claras, de forma que "*los contratistas deben recibir las instrucciones y la formación adecuadas en este sentido*" [516]. Dicha conclusión se encuadra dentro de un planteamiento general, desarrollado por el CICR, en relación con la participación de empresas privadas, en distintas áreas del conflicto. Algunos autores han cifrado esta participación en seis áreas concretas, considerando así, "(…) *The six main roles of business in war: Business as perpetrator, Business as victim, Business as supplier, Business as humanitarian actor, Business as peacebuilder, Business and conflict prevention* (…)[517]

Con independencia de cuantas y cuales sean las concretas funciones, desempeñadas por las entidades privadas, durante el conflicto, es lo cierto que esta circunstancia supone una realidad, a la que debe darse una respuesta jurídica actualizada. Sin embargo, de lo anterior no puede concluirse que, la participación de empresas en el conflicto, sea una circunstancia deseable. Antes bien, para el CICR la presencia de empresas en el conflicto, debería ser restringida, por cuanto "*diversifica e incrementa el número de portadores de armas que*

515 Así se expresa BEERLI, C., La privatización de la guerra: una perspectiva humanitaria. 14 de septiembre de 2012. Declaración de la 35º Mesa Redonda sobre Problemas Actuales de Derecho Internacional Humanitario. San Remo, 6-8 de septiembre de 2012. CICR. https://www.icrc.org/spa/resources/documents/statement/2012/privatization-war-statement-2012-09-06.htm. Fecha de consulta enero de 2013.

516 BEERLI, C., *La privatización de la guerra*, doc. cit.

517 SLIM, H. *Business actors in armed conflict: towards a new humanitarian agenda*. International Review of the Red Cross, vol. 94, no. 887, Autumn 2012; pp. 903-918, en concreto, pp. 912-916.

representan una amenaza para los civiles. Además, contribuye a difuminar la línea esencial que separa a los civiles de los combatientes[518]". No puede olvidarse aquí que, incluso la aplicación del DIH a los Estados, ha planteado problemas de interpretación de las normas, a la luz de los nuevos métodos de combate y formas de conflicto. De este modo, la participación de agentes no estatales plantea retos todavía mayores, en relación al encuadramiento jurídico de su conducta.

El CICR se manifiesta contrario a la contratación de "*personal de las empresas militares y de seguridad privadas para que participe directamente en las hostilidades, incluso si el DIH no lo prohíbe en forma explícita*[519]". Sin embargo, resulta útil en este aspecto, analizar el régimen jurídico aplicable a dichas empresas, al objeto de tomarlo, como referencia para proponer una sujeción, a las normas de DIH, respecto de las empresas privadas que, en el ámbito tecnológico, van a desarrollar un papel decisivo, incluso en el combate. Es decir, el CICR no se ha pronunciado de modo negativo, en cuanto a la contratación de expertos, asesores o proveedores de servicios informáticos. Sin embargo, hay que tener en cuenta que los mismos van a estar presentes, en ocasiones, n unión al Mando militar. En otras ocasiones, van a ser los responsables de la gestión de determinados servicios, que pueden verse afectados por un ciberataque armado.

Como consecuencia de la preocupación por el incremento de entidades mercantiles, presentes en los conflictos armados, prestando esta variedad de servicios, se llegó al compromiso, reflejado en el Documento de Montreal suscrito en 2008[520], que se centra en las obligaciones de los Estados en relación al cumplimiento del DIH. La culminación del proceso ha sido la adopción de los principios guía de Naciones Unidas en negocios y Derechos humanos por el

518 BEERLI, C., *La privatización de la guerra*, doc. cit.
519 *Ibidem.*
520 Documento de Montreux sobre las obligaciones jurídicas internacionales pertinentes y las buenas prácticas de los Estados en lo que respecta a las operaciones de las empresas militares y de seguridad privadas durante los conflictos armados. Anexo de la carta de fecha 2 de octubre de 2008 dirigida al Secretario General por el Representante Permanente de Suiza ante las Naciones Unidas, aprobada por la Asamblea General y el Consejo de Seguridad de Naciones Unidas, en su Sexagésimo tercer período de sesiones y Sexagésimo tercer año. Doc. A/63/467–S/2008/636.

Consejo de Derechos Humanos en 2011[521]. El objetivo de las actividades relacionadas con el conflicto, en las que participan los civiles, hoy no tienen precedente[522]. En el Documento de Montreal queda establecido que la responsabilidad principal de los Estados, consiste en hacer respetar el DIH[523]. En consecución de dicho objetivo, diferentes representantes del sector de las empresas militares y de seguridad privadas adoptaron un Código de Conducta Internacional ayudar a fortalecer el respeto del DIH[524]. Por su parte, el CICR recalca que no incumbe exclusivamente a los Estados el cumplimiento del DIH sino a cualquier agente implicado en el conflicto armado, de modo que dicho cumplimiento exigible a los grupos armados organizados, tanto como a los soldados y a todos "*los actores cuyas actividades estén estrechamente relacionadas con un conflicto armado*[525]."

En estrecha unión se encuentra el concepto de participación directa en las hostilidades, que será objeto de atención, con más detenimiento, en el epígrafe posterior. No obstante, ha de hacerse aquí referencia, aun de forma sumaria, al hecho de que protección otorgada al personal civil, a través del cumplimiento de la obligación de distinguir, entre objetivos militares y civiles y la de atender a la necesidad militar del objetivo que se persigue, entre otras de las ya vistas en el capítulo Segundo, se perderá si, por parte de dicho personal civil, se participa directamente en las hostilidades[526]. El PA I, establece que "*En caso de duda acerca de si un bien que normalmente se dedica a fines civiles, tal como un lugar de culto, una*

521 Estos principios guia son los recogidos en el documento de Naciones Unidas, Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework. United Nations. Human Rights Office of the High Commissioner. New York and Geneva 2011.

522 Second Expert Meeting on the Notion of Direct Participation in Hostilities. The Hague, 25 / 26 October 2004. Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees Expert Paper submitted by Michael N. Schmitt; pp.1-25, en particular, p. 1.

523 El citado Documento de Montreal comienza precisando que "*se recuerdan las obligaciones jurídicas vigentes de los Estados y de las EMSP y su personal (…), y se pone a disposición de los Estados un conjunto de buenas prácticas destinado a promover el respeto del derecho internacional humanitario y de las normas de derechos humanos durante los conflictos armados*".

524 Asi se pone de manifiesto en el documento, BEERLI, C., *La privatización de la guerra*, doc. cit.

525 Así se afirma en el documento publicado por el CICR, *Empresas y Derecho Internacional Humanitario. Introducción a los derechos y las obligaciones de las empresas comerciales, de conformidad con el Derecho Internacional Humanitario*. Comité Internacional de la Cruz Roja, 2006; p.14.

526 El apartado 3 del artículo 51 del PA I, expresamente establece que "*Las personas civiles gozarán de la protección que confiere esta Sección, salvo si participan directamente en las hostilidades y mientras dure tal participación*".

casa u otra vivienda o una escuela, se utiliza para contribuir eficazmente a la acción militar, se presumirá que no se utiliza con tal fin[527]". Sin embargo, los bienes comerciales que se utilicen con fines militares son un objetivo militar y pueden ser legítimamente atacados por las partes en conflicto[528].

Pues bien, en este sentido, para RODRIGUEZ-VILLASANTE Y PRIETO el hecho de acompañar a las Fuerzas Armadas no priva al sujeto de su condición civil, por más que suponga, en un momento dado, el reconocimiento del estatuto de prisioneros de guerra. De este modo, a juicio del autor, "*la noción de participación directa en las hostilidades de estos empleados depende de los mismos criterios aplicables a las restantes personas civiles*[529]".

Sin embargo, ese reconocimiento, como personas civiles, debe ser reconsiderado, en orden a no permitir el abuso, de tal condición, por parte de las empresas y de los Estados para los que éstas trabajan. Es decir, el estatuto de no combatiente ofrece un régimen jurídico, que resulta especialmente protector, del personal civil, como no puede ser de otra manera en un conflicto armado. Sin embargo, es preciso alertar del hecho de que, no sería conforme con el espíritu de la norma y la práctica de los Estados, que esta protección alcanzara a abusa de ella, para desarrollar determinadas funciones, ligadas al combate. En determinadas ocasiones, una conducta de tal índole podría ser calificada, jurídicamente, como pérfida, en función de los criterios, a los que ya se hizo alusión, al analizar el contenido de la obligación jurídica internacional violada. Se trata, por lo tanto, aquí, de evitar que, las empresas que prestan servicios de red realicen actividades, que pudieran beneficiar a la Parte combatiente, prevaliéndose de su condición civil.

Por otra parte, no parece que sea imprescindible la incorporación de este personal, ya sea formalmente, bien de facto, a las Fuerzas Armadas, para que sea posible realizar una "*función permanente de combate*". Tampoco que, únicamente, de esa forma, se pierda dicha protección, pues podrá ocurrir, en numerosos casos,

527 Articulo 51 de PA I.
528 Asi puede leerse en *Empresas y Derecho Internacional Humanitario*, doc. cit.; p.17.
529 RODRÍGUEZ-VILLASANTE Y PRIETO, J. L., *La pérdida de la inmunidad de las personas civiles por su participación directa en las hostilidades,* op. cit.; p. 192.

que dicha función de combate se preste de forma puntual, motivo por el que, en ese momento el personal civil no debería gozar de esa protección. Si se comparte la opinión del CICR, relativa a la inconveniencia de que, el personal civil participe, en gran medida en las hostilidades, una medida disuasoria sería la adopción de un criterio contrario al expuesto. Es decir, que en el momento de realizar cualquier actuación, que contribuya al combate, ese personal civil, esté o no incorporado a las FAS combatientes, pierda su protección.

Pues bien, la participación de las empresas privadas. de una u otra forma. en el conflicto, dista mucho de haber alcanzado un régimen jurídico, más allá del compromiso de Montreal, cuando, lo cierto es que, sus funciones son, cada vez, más diversas.

En el ámbito que aquí nos ocupa, podrá ocurrir que la actuación de una empresa privada conlleve la exigencia de responsabilidad internacional del Estado en dos supuestos.

El primero de ellos de dará cuando, a través de dicha empresa, el Estado dirija un ataque informático, en el ámbito de un conflicto bélico. Podría ocurrir que, como más arriba se ha expuesto, determinados Estados contraten los servicios de asesores, que tengan como cometido el desarrollo de ciberoperaciones, en caso de conflicto armado, a falta de un Mando específico de Ciberdefensa, o en conjunción con el mismo. En este caso, queda claro que dicha actuación entraría de lleno, en el supuesto de los actos realizados, por una entidad privada, bajo la apariencia de las funciones gubernamentales y, en cualquier caso, bajo la dirección o control del Estado. También el Manual de Tallin se pronuncia de forma favorable a dicha tesis, al entender que, en este supuesto, incurriría en el contenido del artículo 8 del Proyecto, por tratarse de una conducta, realizada al amparo del Derecho Internacional, en los supuestos en que "*la persona o grupo actúen de hecho bajo instrucciones o bajo la dirección o control del Estado que desarrolla la conducta*"[530].

En conclusión, parece evidente que el régimen jurídico que, con carácter general, pretende aplicarse a las empresas de seguridad, debería, también, ser

530 SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p.37.

aplicado a las empresas tecnológicas o de comunicaciones, que prestan servicios de internet, de forma que se evite la "*elusión de responsabilidades y la impunidad de los infractores*[531]". Como también justifica GARCIA SEGURA, ello ha de hacerse, a través de la actuación de los Estados, habida cuenta su condición de contratistas mayoritarios de los servicios, prestados por estas empresas. Además, puede compartirse con el autor que, como ya se ha aludido en este Capítulo, los Estados ostentan el monopolio del uso legítimo de la fuerza y, por último "*porque* (los Estados) *son responsables ante los ciudadanos, a quien les une el mandato democrático, de la defensa de los valores y principios que proclaman; y porque sólo a través de ellos, pueden ejercer presión sobre las empresas ya que en el caso de las EMSP ni siquiera adquieren sus servicios*[532]". Por lo tanto, en aquéllos supuestos, en que pueda acreditarse una actuación, por parte de una empresa, de la naturaleza que aquí se ha tratado y, que sea consecuencia de los mandatos del Estado, esa conducta deberá ser atribuida al Estado de que se trate.

Por otra parte, si los contratistas y empleados civiles son incorporados a las Fuerzas Armadas, "*a través de un procedimiento oficial de conformidad con el derecho interno*" o bien "*de facto porque se les ha asignado una función continua de combate*", ya no puede entenderse que este personal sea civil, sino combatiente. En aplicación de las pautas contenidas en la Guía, las "compañías militares privadas", pueden llegar a ser partes no estatales, independientes en un conflicto armado no internacional. Pues bien, en el caso de que dicha situación se verificara en un conflicto armado internacional, habría que aplicar idéntica conclusión.

En conclusión, el hecho de que, en los conflictos armados internacionales y no internacionales, participen agentes externos a los Estados, no puede evitar la responsabilidad de quien, directamente, comete los hechos ni de los Estados que, de uno u otro modo, se valen de esos agentes, es decir, las compañías privadas,

531 GARCÍA SEGURA, C., *Las iniciativas para la regulación de la actividad de las empresas militares de seguridad privada*. Las corporaciones privadas de seguridad. Plan Anual de Investigación 2015. Documento de trabajo 13/2015. Escuela Superior de las Fuerzas Armadas; pp. 14-38, en particular, p.36.

532 GARCÍA SEGURA, C., *Las Las iniciativas para la regulación de la actividad de las empresas militares de seguridad privada*, op. cit.; p.36.

para cometer el hecho ilícito. Esta conclusión, por otra parte parece necesaria, pues como manifiesta KYRIAKAKIS, la participación del sector privado se manifiesta de muy diversos modos, entre los que puede encontrarse, también, la violación de derechos[533].

4.1.2.- El papel de las empresas que conforman las infraestructuras críticas como víctimas de un ciberataque.

Si, hasta ahora, se ha analizado el papel de las empresas que, de un modo u otro, van a actuar prestando un servicio al Estado, en este momento es necesario abordar otro de los papeles que podrá, presumiblemente, desempeñarse en los conflictos contemporáneos. Actaulemnte, hay que asumir que los conflictos podrán ofrecer una nueva perspectiva, en cuanto a la participación del personal civil por cuanto, en ellos, "*serán objetivo los negocios civiles altamente valuados*" y esto conducirá a que "*Los Estados nación entonces, necesitarán integrar a los empleados civiles de esas y quizás otras compañías en sus estructuras de respuestas a su ciberguerra si el Estado es capaz de responder efectivamente a los ciberataques*[534]".

Como se viene poniendo de manifiesto, en el presente Capítulo, se trata de analizar una serie de cuestiones que, con toda probabilidad, serán frecuentes para gran parte de Estados. En países como los Estados Unidos, resulta habitual que las infraestructuras sean compartidas por el personal civil y el militar y que, las comunicaciones militares utilicen redes, que son propiedad del sector privado que, a su vez, presta ese mismo servicio al personal civil.[535]

---

533 En este sentido el autor entiende que "*With increasing awareness that economic concerns and actors have a central part in many modern conflicts – as financiers and enablers of violence, as direct actors in the case of private military companies, and as partners of rights violating security forces – the demand that international criminal law evolve to address the business dimensions of conflict is likely to continue. After all, international criminal law has as one of its key goals and justifications the furtherance of peace and security*". KYRIAKAKIS, J. *Developments in international criminal law and the case of business involvement in international crimes.* Business, violence and conflict. International Review of the Red Cross, vol. 94, no. 887. Autumn 2012; pp. 981-1005, en particular, p.1004.

534 BRENNER, S. W. with CLARKE, L. L. *Civilians in Cyberwarfare: Conscripts*, op. cit.; p.1037.

535 Así lo pone de manifiesto LIN quien, además en este mismo sentido, expone que atendiendo a muchas interpretaciones del DIH, la dependencia militar de la infraestructura civil hace que la infraestructura civil sea un objetivo legítimo (un objeto de doble uso) para las operaciones

Entre las empresas que pueden verse en dichas circunstancias, hay que hacer una especial referencia a aquellas que se dedican a la prestación de servicios tecnológicos y, además, son propiedad del Estado. Aunque, como señalan SCHMITT y VIHUL, el criterio de la propiedad de la compañía no puede ser determinante, en el momento de atribuir el hecho ilícito al Estado[536].

La dificultad en la atribución de la conducta se dará en los supuestos en que, determinadas empresas, sean objeto de ciberataques. Si bien es cierto que el contexto, que aquí se analiza, está basado en la existencia de un conflicto bélico y en el desarrollo de las cibeoperaciones, durante el mismo, es igualmente reseñable, el hecho de que dicho conflicto va a presentar una serie de rasgos diferenciados del conflicto tradicional que, nuevamente, habrá que tener en cuenta. Ya se ha hecho mención en la Primera parte del presente trabajo a dos situaciones que aquí vuelven a tener protagonismo: el conflicto híbrido y los ciberataques como potenciadores de un conflicto armado. En este sentido, hay que recordar que, el modo en que, actualmente, se desarrollan los conflictos dista mucho de la tradicional concepción, que se tiene de los mismos y que, el ataque a determinados objetivos civiles, puede resultar frecuente en el futuro. Así, es probable prever el supuesto de una empresa privada, perteneciente al ámbito de las infraestructuras críticas, que resulte víctima de un ataque armado cibernético y que, dicha empresa, se encuentre en la necesidad de responder a dicho ataque.

Es el caso que ya quedó apuntado en la Primera Parte, en relación a los ataques sufridos por la empresa estadounidense Sony. Es evidente que dicho ataque no revistió la gravedad, ni demás características apuntadas en el dicho Capítulo para ser tenido por un ataque armado[537]. No obstante, puede servir de

militares del adversario. LIN, H., *Cyber conflict and international humanitarian law*. Humanitarian debate: Law, policy, action. New technologies and warfare. International Review of the Red Cross, vol. 94, no. 886. Summer 2012; pp.515-531, en particular, p.528.

536 En este sentido, SCHMITT y VIHUL entienden que "*Ownership by the state as such does not suffice for attribution. Instead, a company (assuming it is not exercising elements of governmental authority) must be acting under the instruction, direction, or control of the state before its cyber activities are attributable to that state*". SCHMITT, M., N. & VIHUL, L., *Proxy Wars in Cyberspace*, op. cit.; p.62.

537 SCHMITT, al respecto afirma, "*Albeit highly disruptive and costly, such effects are not at the level most experts would consider an armed attack. Additionally, some States and scholars reject the view that the right of self-defense extends to attacks by non-State actors. Even though the attribution of the Sony incident to North Korea has been questioned, this debate is irrelevant because the operation failed to qualify*

referencia, porque puede llegar a repetirse un ciberataque en las mismas circunstancias y podrá ser dirigido contra una empresa, que forme parte del sistema de infraestructuras críticas. El ataque a la empresa Sony ha sido considerado, por parte de la doctrina internacionalista, como una violación de la soberanía de los Estados Unidos y así, SCHMITT entiende aplicable el Proyecto, en virtud de la violación de la obligación internacional de respetar dicha soberanía[538].

Mientras la Comunidad Internacional se ha centrado en tratar las empresas militares de seguridad vía el Proceso de Montreal y el Código de Conducta Internacional para los Proveedores de Seguridad privada, la industria ha evolucionado, nuevamente, de tal manera que este proceso podría quedar sin efecto. Más aun, ambos documentos, el de Montreal y el aludido Código quedan como acuerdos voluntarios y representan un cambio hacia la autoregulación, que ha ocurrido, parcialmente, a causa de la inhabilidad de las partes relevantes, para idear una regulación formal.[539]

En este caso, podremos encontrarnos ante diversas situaciones. Así, si una empresa privada, dedicada a cualquiera de las actividades, propias de los sectores económicos, que se recogen en el anexo de la Ley de Protección de Infraestructuras Críticas, es víctima de un ciberataque armado, podrá suceder que, ante la virulencia del ataque se respondiera por parte de las Fuerzas Armadas, si esa conceptuación del ataque, como ataque armado es evidente. No obstante, podrá también suceder que la empresa responda, por sí misma, para defenderse. No puede olvidarse que, al margen de la existencia de un conflicto

---

as an armed attack in the first place". SCHMITT, M., N. International Law and cyber attacks: Sony v. North Korea. Disponible en el sitio web: www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea. Fecha de consulta, junio 2016.

538 La cuestión de la atribución, no obstante, sigue aquí latente, de modo que el autor la analiza entendiendo que "*To constitute a breach of sovereignty, an action must be attributable to a State. If North Korea's Bureau mounted the cyber operation, there is no question of attribution since its hackers work for the military's General Bureau of Reconnaissance, and therefore are State "organs" whose actions are, as recognized in Article 4 of the ILC's Articles on State Responsibility, attributable to North Korea (even if acting ultra vires). If conducted by a non-State group, attribution for the operation would attach only if North Korea directed and controlled it (Article 8), or later acknowledged and adopted the action as its own (Article 11)*". SCHMITT, M., N. *International Law and cyber attacks: Sony v. North Korea*, op. cit.

539 PERCY, S. *Regulating the private security industry: a story of regulating the last war*. International Review of the Red Cross, vol. 94, no. 887. Autumn 2012; pp.941-960, en particular, p. 945.

armado, la legítima defensa, ante una agresión ilegítima, está garantizada por la legalidad interna e internacional. En este ultimo supuesto, podría darse el caso de que la empresa incurriera en un excedso, provocando con su inadecuada respuesta un ataque desproporcionado o indiscriminado o, cualquier otro, que violara norma de DIH.

Pues bien, en este último supuesto se dará el caso de una empresa privada que no actua para las Fuerzas Armadas de un Estado, es decir que no es un contratista y que tampoco actúa ejerciendo funciones que podrían llamarse gubernamentales. Por lo tanto, en principio, habrá de quedar al margen de la aplicación del artículo 8 del Proyecto, hasta ahora estudiado. Sin embargo, cabe plantearse si la respuesta, ofrecida por la empresa, y las actuaciones subsiguientes entrarían en el concepto de "función continua de combate". No es lejano a la realidad que, en el futuro se produzcan situaciones similares y que, de uno u otro modo, el Estado pretenda ejercer un control respecto de la respuesta que se ofrezca[540].

En el caso español, la necesidad de proteger las infraestructuras críticas ha sido reflejada en la normativa interna, de modo tal que, dicha necesidad que podríamos considerar de índole práctica o material, ha pasado a ser una obligación de naturaleza jurídica. En consecuencia, tanto la Ley 8/2011 de Protección de las Infraestructuras Críticas, como el Real Decreto 704/2011, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, articulan un complejo sistema interdepartamental, para la protección de las mismas, compuesto por órganos y entidades pertenecientes, a las Administraciones Públicas y al sector privado[541].

---

540 BRENNER y CLARKE ofrecen un hipotético ejemplo en los Estados Unidos en los siguientes términos: "*If U.S. computer systems become the targets of large-scale cyberwar attacks, the military probably will not want to leave the defense of those and other systems to the idiosyncratic efforts of autonomous civilians. The military will probably want to control and coordinate the responses – offensive as well as defensive – that are used to protect U.S. systems. The logical way to control the responses is to somehow control civilians who have the ability to battle cyberattackers*". BRENNER,S.W. with CLARKE, L. L., *Civilians in Cyberwarfare: Conscripts*, op. cit.; p. 1037.

541 Además, este sistema diseña un planeamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación. Por otra parte, sirve a los fines del Sistema Nacional de Gestión de Situaciones de Crisis y cumple

La Ley 8/2011 cataloga el conjunto de las infraestructuras, que prestan servicios esenciales para la sociedad y diseña un planeamiento de medidas de prevención y protección, contra las posibles amenazas, tanto en el ámbito de la seguridad física, como en el de la seguridad de las tecnologías de la información y las comunicaciones. Como consecuencia de ello, la Secretaría de Estado de Seguridad, del Ministerio del Interior, ha aprobado el primer Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007 y ha elaborado el primer Catálogo Nacional de Infraestructuras Estratégicas. Resulta esencial en este punto recordar la necesidad de coordinación, entre el sector público y el privado, por el que se abogaba en epígrafes precedentes pues, en este ámbito, ya se establecen las medidas de protección de las infraestructuras críticas, que proporcionan una base adecuada para la coordinación de las Administraciones Públicas y de las entidades y organismos, gestores o propietarios, de infraestructuras que presten servicios esenciales para la sociedad.

De este modo, la seguridad cibernética de las infraestructuras críticas no es recogida, únicamente, en documentos de carácter técnico o político sino que, como afirma CARO BEJARANO, "*existe ya una normativa con rango de ley sobre la que se sustentan dichas iniciativas, que establece con claridad las responsabilidades y obligaciones de los diferentes agentes involucrados en su protección a nivel nacional*[542]."

Es el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, el que detalla dichas responsabilidades, concernientes a cada uno de los operadores implicados en la protección de estas infraestructuras[543]. Es decir que, en el ámbito de la protección

---

con la transposición obligatoria de la Directiva 2008/114/CE, del Consejo de la Unión Europea, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. Así puede leerse en la Exposición de Motivos del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Publicado en BOE núm. 121, de 21 de mayo de 2011.

542 Así se expresa CARO BEJARANO, al abordar el análisis de la ley 8/2011, en CARO BEJARANO, M. J. *La protección de las infraestructuras críticas*. Documento de Análisis 021/2011, 27 de julio de 2011. Instituto Español de Estudios Estratégicos; p. 3. Disponible en el sitio web:http://www.ieee.es/Galerias /fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf. Fecha de consulta, marzo de 2013.

543 De esta forma, al Ministerio de Interior, a través de la Secretaría de Estado de Seguridad corresponde, entre otras, las funciones de identificar los diferentes ámbitos de responsabilidad en

de las infraestructuras cibernéticas el nivel de seguridad que determina la ciber-resiliencia[544] será escrutado por la Secretaría de Estado. Por su parte, al Centro Nacional para la Protección de las Infraestructuras Críticas se le encomienda, entre otras tareas, las de ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas y irigir y coordinar los análisis de riesgos, que se realicen por los organismos especializados, públicos o privados, sobre cada uno de los sectores estratégicos.

A su vez, el Ministerio de Defensa no se encuentra ajeno, por completo a la responsabilidad, concerniente a la protección de infraestructuras críticas. Antes bien, el apartado 2 del artículo 5 de la misma Ley establece que son *agentes del Sistema*, con las funciones que se determinen reglamentariamente, (…) *c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley* y aparece relacionado hasta por tres veces en dicho Anexo. En concreto el Ministerio de Defensa aparece en relación con las Tecnologías de la Información y las Comunicaciones (TIC), la Administración y el Espacio.

Pues bien, este régimen jurídico que aquí se indica, establece que son doce los sectores estratégicos que, a su vez, se hallan subdivididos en subsectores, ámbitos y segmentos y que recogen los servicios que se consideran esenciales para la sociedad. Estos doce sectores son los siguientes: Administración, Alimentación, Energía, Espacio, Sistema Financiero y Tributario (por ejemplo,

---

la protección de infraestructuras críticas. Para ello está encargado de analizar los mecanismos de prevención y respuesta previstos por cada uno de los actores implicados; emitir las instrucciones y protocolos de colaboración dirigidos tanto al personal y órganos ajenos al Ministerio del Interior como a los operadores de las infraestructuras estratégicas, así como, fomentar la adopción de buenas prácticas y, por último, responder del cumplimiento de las obligaciones y compromisos asumidos por España en el marco de la Directiva 2008/114/CE, sin perjuicio de las competencias que corresponden al Ministerio de Asuntos Exteriores y de Cooperación. Así puede leerse en el artículo 6 del Real Decreto 704/2011.

544 La ciber-resiliencia, será ese nivel óptimo de seguridad con el que ha de contar una organización, que pretenda evitar un ciberataque y las medidas de reacción y superación del mismo, una vez sufrido. El concepto aparece en el primer lugar de la lista de las cinco prioridades y medidas del documento de Estrategia de Ciberseguridad de la Unión Europea. Comunicación conjunta al Parlamento Europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. El documento de la Unión Europea es citado por DE SALVADOR CARRASCO, L., en *Ciber-resiliencia*. Documento de opinión 35/2015, de 3 de abril de 2015. Instituto Español de Estudios Estratégicos; p.5. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf. Fecha de consulta, julio de 2015.

banca, valores e inversiones), Agua (embalses, almacenamiento, tratamiento y redes), Industria Nuclear, Industria Química, Instalaciones de Investigación, Salud, Tecnologías de la Información y las Comunicaciones y Transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico). Es decir, aquéllos servicios críticos, a los que el capítulo 4 de la Estrategia Española de Seguridad ya, en el año 2011[545] (en adelante, EES) citaba y, respecto de los que puntualizaba que,

> "fenómenos naturales extremos, atentados terroristas o ciberataques, entre otros de las amenazas y riesgos analizados, pueden dañar las infraestructuras críticas, suministros y servicios críticos que sustentan nuestra vida y el desenvolvimiento de nuestra sociedad. Debemos proteger y garantizar su normal funcionamiento para no perjudicar el bienestar y la economía de un país avanzado como el nuestro".

Como en repetidas ocasiones se ha puesto de manifiesto, no nos encontramos ante una situación aislada, sino antes bien, ante circunstancias concurrentes, en gran parte de los Estados, con los que España comparte intereses en el ámbito de la Defensa[546]. Así, en el caso de los Estados Unidos, algunos autores han considerado que solo con la colaboración de los actores no estatales apropiados, es posible lograr la resiliencia del ecosistema[547]. Asimismo, la dependencia militar, de determinadas infraestructuras civiles, fundamenta la

545 Estrategia Española de Seguridad. Una responsabilidad de todos. Gobierno de España. 2011; pp.41-79.

546 Al respecto, DION, expone que "*In the United States, critical infrastructure includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*" "*In Australia, "[c]ritical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security*". DION, M., *Different Legal Constructs for State Responsibility.* International Cyber Security Legal & Policy Proceedings 2010. NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn, 2010; pp. 67-75, en particular, p. 68.

547 RATTRAY y HEALEY justifican tal afirmación al entender que "*stopping attacks even from small groups often requires coordinated actions by defenders in both state and non-state organizations who may have little trust and few incentives to cooperate*". RATTRAY, G. J. and HEALEY. J. *Non -State Actors and Cyber Conflict. America's Cyber Future,* op. cit, p.68.

preocupación por el ataque que, éstas pudieran sufrir, pues ello permitiría al atacante erosionar la operatividad interna[548].

Como afirma CARO BEJARANO, la Ley 8/2011, aborda la protección de las infraestructuras, de modo que quedan considerados, en la misma, todos tipos de amenazas, incluidas las virtuales.[549] RAMIREZ MORAN, por su parte, pone de manifiesto que, en Europa, un elevado porcentaje de países cuenta con un documento de esta naturaleza. En Norteamérica Estados Unidos y Canadá cuentan, también, con su propia estrategia de ciberseguridad[550].

Pues bien, una vez recibido un ciberataque, por parte de una de las empresas, que gestione una actividad, incluida en alguno de los sectores estratégicos, cabe preguntarse si el comportamiento de dicha empresa, al repeler el ataque puede ser atribuido al Estado cuando dicha empresa actue, de manera incompatible, con las obligaciones internacionales del Estado interesado. Al respecto, el Comentario al artículo 8 del Proyecto recuerda que el Derecho Internacional "*reconoce la identidad separada de las personas morales en el ámbito nacional*[551]", de forma que la pertenencia al Estado de la compañía "*no constituye base suficiente para atribuir al Estado el comportamiento ulterior de esa entidad*[552]", como ya ha sido anteriormente señalado. Antes bien, el Comentario al Proyecto establece que las sociedades, aun siendo propiedad del Estado, "*se consideran entidades separadas, a primera vista su comportamiento en el curso de sus actividades no es atribuible al Estado, a menos que ejerzan atribuciones del poder público en el sentido del artículo 5*"[553].

548 BRENNER y CLARCKE, por su parte, afirman que "*an attack can deprive the victim state of infrastructure that supports military actions*". BRENNER, S. W. with CLARKE, L. L. *Civilians in Cyberwarfare: Conscripts*, op. cit.; p. 1029.

549 Así se expresa CARO BEJARANO, al abordar el análisis de la ley 8/2011, en CARO BEJARANO, M. J. *La protección de las infraestructuras críticas,* op. cit.; p.7.

550 RAMIREZ MORAN puntualiza que, que únicamente Portugal, Islandia, Suiza, Eslovenia, Bosnia, Serbia, Croacia, la ex-república yugoslava de Macedonia, Albania, Bulgaria, Moldavia, Ucrania y Bielorrusia, quedan fuera de esta lista. RAMÍREZ MORÁN, D., *La visión internacional de la ciberseguridad*. Documento Informativo 2/2015, de 1 de abril de 2015. Instituto Español de Estudios Estratégicos; p. 5. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf Fecha de consulta, junio de 2015.

551 Comentario 6) al articulo 8 del Proyecto.

552 Comentario 6) al articulo 8 del Proyecto.

553 Comentario 6) al artículo 8 del Proyecto.

En consecuencia, será preciso determinar si, ese personal goza del estatuto de combatiente, con todas sus garantías, de modo que el Estado, responda de las violaciones de obligaciones de DIH que se cometan por dicho personal o, por el contrario, se trata de personal, cuya condición civil, impide la entrada en combate y deslegitima cualquier ataque sufrido por ellos, por no tener la condición de objetivo militar. Por lo tanto, la situación en la que puede encontrarse una empresa, que gestione una actividad, comprendida dentro del sector de las infraestructuras críticas, puede ser muy similar a la de las Fuerzas Armadas. En consecuencia, será aconsejable determinar, con antelación, si nos encontramos ante la actuación de personal civil o por el contrario, el personal de la empresa en cuestión, goza del estatuto de combatiente, mientras desempeñe tales misiones.

De forma evidente estas cuestiones exceden el ámbito del papel de las empresas en el conflicto armado, al menos, tal y como ha sido conceptuado hasta el momento. Estos interrogantes entran, de lleno, en la polémica relativa a la participación de civiles en las hostilidades. Es decir, con independencia de su pertenencia o no a una corporación mercantil, el personal civil, podrá comprometerse con un objetivo militar a través de la red de diversas formas.

A la luz de los Convenios de Ginebra, podemos encontrarnos con las categorías de combatientes legítimos e ilegítimos y, en tercer lugar, el personal civil, es decir, personas que, en palabras de BRENNER y CLARKE, "*do not qualify as combatants under the Geneva Convention standards and did not take an active role in carrying out military hostilities*[554]". Sin embargo, como también apuntan los autores, dichos Convenios responden a la necesidad de regular una serie de situaciones en las que, de modo predominante, el personal militar se encargaba del desarrollo del conflicto, mientras que el civil sufría las consecuencias de la guerra y, por lo tanto, debía de ser acreedor de una eficaz protección frente a sus consecuencias. En conclusión, a juicio de los mismos autores, los Convenios no son susceptibles de aplicación «*to corporations and other artificial entities. They may,*

554 BRENNER, S. W. with CLARKE, L. L. *Civilians in Cyberwarfare: Conscripts*, op. cit.; pp. 1022-1023.

however, reach a corporation's "conduct as violative of customary international law." »[555].

La Guía, por su parte, deja sentado que el personal civil, constituido por contratistas privados y empleados, no puede perder tal condición, en tanto no se halle incorporado a las Fuerzas Armadas de un Estado. Asimismo, afirma que cuando dichas personas, "*participen directamente en las hostilidades, sin la autorización expresa o tácita del Estado parte en conflicto siguen siendo civiles y pierden la protección contra los ataques directos mientras dure su participación directa*[556]". Por lo tanto, la participación directa asimila a estos civiles a los combatientes. Esta circunstancia, a juicio de algunos autores, debería producirse de forma obligatoria, en el sentido de que determinadas personas, deberían ser, incluso, reclutadas imperiosamente para la defensa de las infraestructuras críticas del Estado[557].

En el caso español, el Estado responsable, en todo caso, será el español pues la Ley 8/2011 no hace distinciones, en cuanto a la nacionalidad de la sociedad o, al Estado de origen de la empresa. Respecto de las empresas insertas en el catálogo de Infraestructuras Críticas, la Ley establece una serie de obligaciones, de cuya ejecución se encarga, asimismo, el Estado, a través de la Secretaría de Estado de Seguridad, del Ministerio del Interior[558]. Es decir, el artículo 5 de la Ley anticipa los responsables de la gestión de seguridad, del sistema de infraestructuras críticas. En función del lugar de la cadena de agentes

555 BRENNER, S. W. with CLARKE, L. L. *Civilians in Cyberwarfare: Conscripts*, op. cit.; pp. 1022-1023.

556 MELZER, N., S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p. 39.

557 "*Civilians administering critical infrastructure who use active defenses to respond to a cyber operation might be categorized as a cyber levée en masse, and thereby entitled to combatant status*". PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*, op. cit., p. 294.

558 La Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas, enumera como agentes del Sistema, con las funciones que se determinen reglamentariamente, los siguientes: "*a) La Secretaría de Estado de Seguridad del Ministerio del Interior. b) El Centro Nacional para la Protección de las Infraestructuras Críticas. c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley. d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía. e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía. f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional. g) La Comisión Nacional para la Protección de las Infraestructuras Críticas. h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas. i) Los operadores críticos del sector público y privado*". Artículo 5.2 de la Ley 8/2011, doc. cit.

del sistema, donde se produzca el hecho ilícito, la responsabilidad por el mismo será del Estado. Así, si el hecho ilícito es cometido por alguna de las autoridades enunciadas entre las letras a) hasta la h), parece evidente que el hecho ilícito sera atribuible al Estado, que, en esos casos, estará actuando a través de alguno de sus agentes, bien por acción, bien por omisión. Únicamente parece que el hecho pudiera atribuirse a la empresa, en el caso de hallarse en el supuesto de la letra i) del citado artículo.

No obstante, en el supuesto de que la persona encargada de ejecutar la respuesta al ciberataque, desobedeciera las medidas impuestas en la Ley y sus instrumentos de desarrollo o, incumpliera las indicaciones de la Administración en la gestión de la crisis, caso de haberlas, no podría hacerse responsable al Estado del hecho ilícito cometido bajo dichas premisas.

Por último, cabe concluir que, a la vista de las funciones que se asignan a los operadores críticos, por el artículo 13 del Reglamento de desarrollo de la Ley 8/2011, parece improbable que, el incumplimiento de sus obligaciones pudiera desencadenar una violación de una norma de DIH, salvo en el caso de que, la actuación se realice desatendiendo las instrucciones, dadas expresamente, por la Administración.

4.2. Los cibervoluntarios en el conflicto armado.

Como también se ha anticipado en la primera Parte del presente trabajo, el ciberterrorismo es una de las actividades que, con frecuencia puede encontrarse en la red y que podrá originar confusión, a la hora de su calificación jurídica, por cuanto presenta elementos comunes con los ciberataques cuando éstos sean ataques armados. En este punto, el deslinde con las actividades terroristas en la red, vuelve a resultar oportuno, pues la actividad de los ciber terroristas durante un conflicto armado, debe ser objeto de atención en orden a determinar cuál es el régimen jurídico aplicable a los mismos y, en qué grado o en virtud de qué criterio, su actividad puede ser atribuida a un Estado. En determinadas ocasiones la participación de agentes no estatales será alentada por los propios Estados, de modo que se imposibilite la atribución a dichos Estados de hechos ilícitos que, sin

embargo, responden a sus intereses. Asimismo, los civiles pueden tener interés en participar en un conflicto armado para expresar su apoyo a una de las partes contendientes [559]. La participación de civiles en el lanzamiento de ciber operaciones presenta la ventaja de la dificultad, en la atribución al Estado, del hecho internacionalmente ilícito, pero también la de contar con personal altamente cualificado, que pudiera repeler determinados ciber ataques[560].

Si en el epígrafe anterior ha quedado apuntada la posibilidad de que, de un modo, más o menos forzado, se produzca la participación de personal civil en operaciones cibernéticas, va a ser abordada ahora la cuestión de dicha participación de forma voluntaria por parte de los civiles implicados.

La clandestinidad que ofrece internet podrá ser usada, por los Estados, para eludir su responsabilidad internacional[561] y por los propios internautas, de forma que la participación de los mismos podrá ofrecer una gran cantidad de modalidades, como también exponen SCHMITT y VIHUL, al entender que "*they could include, for example, individual hackers, criminal groups, an informal group with its own identity like Anonymous, a legal entity such as the Microsoft Corporation, or terrorist or insurgent groups*" [562].

Pues bien, en estos supuestos ya no nos encontramos ante personas que por su especial cualificación o por la ocupación de puestos clave en el ámbito privado puedan verse involucrados en tales actividades sino de personas que libremente deciden tomar parte en un conflicto armado internacional o no internacional. Desde este punto de vista, la calificación jurídica de la conducta y el régimen jurídico que aplicable.

La participación de personal civil a través de la realización de ciberactividades de muy diversa índole se trata de un fenómeno que en tiempos recientes está tomando un especial protagonismo, pero cuyo origen se remonta a

559 Así lo ha expresado PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*, op. cit.; p. 291.

560 De este modo, BRENNER y CLARKE abogan incluso por un reclutamiento obligatorio de los civiles que pudieran prestar dicho servició a las Fuerzas Armadas. BRENNER, S. W. with CLARKE, L. L. *Civilians in Cyberwarfare: Conscripts*, op. cit.; p. 1047.

561 SHACKELFORD, S. J., *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, op. cit.; p. 198.

562 SCHMITT, M. N. & VIHUL, L., *Proxy Wars in Cyberspace,* op. cit.; p. 62.

varias décadas atrás. Ya en la década de los 90 del siglo pasado se tuvo conocimiento de actuaciones de esta índole y también a comienzos de la década del 2000[563]. Desde esos comienzos, son múltiples las modalidades que puede presentar la participación de civiles en la red, como se veía en el capítulo precedente, sin poder obviar el hecho de que las distintas motivaciones de cada uno de ellos no tienen por qué ser desarrollada al margen del conflicto armado. Es decir, la actividad en la red, sea lícita o no, puede ser desarrollada por hacktivistas, ciber criminales, ciber espías, y todos aquéllos que han sido previamente enumerados, durante de forma simultánea al desarrollo de un conflicto armado[564]. Por este motivo, la actuación de civiles en la red, durante el conflicto armado debe ser objeto de una especial atención por parte del DIH, pues la atribución de un hecho ilícito a alguno de ellos, en determinadas ocasiones, conllevará la exigencia de responsabilidad internacional del Estado.

4.2.1. La atribución del hecho ilícito cometido por ciberterroristas en el conflicto armado.

En el transcurso de un conflicto armado internacional o no internacional, podra constatarse la actividad de grupos terroristas, a traves de internet que, sin llegar a realizar ese "ciberatentado" del que se hablaba en la Primera Parte del

563 Así, se habla de los primeros *hackers* que actuaron movidos por intereses patrioticos, como los "*Chinese hackers responding to the accidental bombing of the Chinese embassy in Belgrade in 1999 and a collision between Chinese and U.S. military aircraft in 2001. The earliest patriotic hacker campaigns were tracked by Attrition.org, a website that archived defaced web pages from 1995 to 2001.19 Even though Attrition.org was a non-state actor, both military and civilian cyber defenders relied on it to track malicious activity*". RATTRAY, G. J. and HEALEY. J. *Non -State Actors and Cyber Conflict*, op. cit.; p.71.

564 Así lo pone de manifiesto LIN que, al respecto afirma que "*Indeed, some (but only some) such operations can be conducted with information and software found on the Internet and hardware available at any local computer store. Motivations for conducting such operations – that is, for engaging in cyber conflict – also span a wide range. One of the most common motivations today is financial. Another possible reason for such operations is political – the perpetrator might conduct the operation to advance some political purpose. may be conducted to send a political message to a nation, to gather intelligence for national purposes, to persuade or influence another party to behave in a certain manner, or to dissuade another party from taking certain actions. Still another reason for conducting such operations is personal. Lastly, such operations may be conducted for military reasons, in the same way that traditional military operations involving kinetic weapons are used*". LIN, H., *Cyber conflict and international humanitarian law*, op. cit.; pp.519-520.

trabajo, sí que suponga una actividad, lo suficientemente relevante, como para requerir una respuesta jurídica.

Se tiene constancia de que, en los conflictos contemporáneos, la importancia del uso de internet ha crecido, de tal modo que puede afirmarse que, el conflicto armado se libra en dos ámbitos o entornos paralelos: el real y el virtual y que, tan importante es la victoria en el Teatro de Operaciones como en la red. Dicha red, para los "*grupos armados insurgentes en Irak (y en cualquier otro lugar) es utilizada por los yihadistas como vectores para su lucha, dado que Internet constituye su único medio de comunicación con el mundo exterior*[565]". De este modo, el ciberterrorista se convierte, en su propio ámbito, en un elemento de la misma importancia, que el combatiente en el conflicto armado.

Sin embargo, esto no puede llevar a la errónea conclusión de entender que, el conflicto, en algún modo, queda equilibrado, sino que, por el contrario, se pone de manifiesto un elemento conformador de la asimetría del conflicto: la asimetría jurídica[566].

El tratamiento jurídico, que ha sido dado a los ataques terroristas y sus perpetradores, desde el punto de vista del Derecho Internacional, ha sufrido una evolución, a lo largo de la última década, indefectiblemente unida a las actuaciones que siguieron a los atentados, cometidos en los Estados Unidos el 11 de septiembre de 2001. La respuesta de los Estados Unidos, entendiendo que dicho atentado era atribuible al grupo terrorista Al Qaeda, constituye un punto de inflexión, en el tratamiento de los grupos terroristas, que conviene tener presente en este momento[567]. Como consecuencia de dichos sucesos, los Estados

565 Para ADHAMI, "*El uso de una guerra de guerrillas, que el ejército convencional de Estados Unidos enfrenta con dificultad, ha permitido a la insurgencia sunita sabotear los esfuerzos de reconstrucción y cualquier otro plan para establecer y mantener la seguridad en Irak*". ADHAMI, W., *La importancia estratégica de Internet para los grupos armados insurgentes en las guerras modernas*. International Review of the Red Cross núm. 868. Diciembre de 2007; pp. 305-327, en particular, pp. 316-317.

566 SCHMITT, al respecto afirma: "(…) *the most visible influence is that exerted by technological differences in the military power of opposing sides. However, other forms of asymmetry also drive the willingness of participants to abide by the norms of IHL, or, perhaps more precisely, deviate from them*." SCHMITT, M., N. *Asymmetrical warfare and International Humanitarian Law*. Air Force Law Review, vol. 62, no. 1, 2007; pp. 2-42, en particular, p.41.

567 Así lo entiende VITÉ que considera que "*in certain contexts the fight against terrorism may also take the form of an armed conflict. That is the case when it results in a clash between States, as was the case when the United States of America attacked Afghanistan in October 2001. That fight may also be the*

Unidos invocaron su derecho a la legítima defensa, conforme al artículo 51 de la Carta de Naciones Unidas[568]. No procede aquí tratar las consecuencias jurídicas de dicha decisión, por cuanto serán objeto de estudio en el Capitulo siguiente, al abordar la legitima defensa, pero si advertir de las consecuencias de la intervención terrorista en los conflictos armados.

La necesidad de aplicar el DIH a los conflictos, que se libran entre Estados y entidades no estatales, ya había sido demostrada, a juicio de algunos autores, con anterioridad a dicho ataque terrorista y, para éstos, se trató de una nueva concepción de ataque armado, aunque "*no en el sentido entendido tradicionalmente por la Carta*"[569]. Sin embargo, como pone de manifiesto MORENO FERNANDEZ, la atribución a Afganistán del atentado cometido por Al Qaeda no es posible ni siquiera aplicando la teoría del control general. En todo caso, podría entenderse que en un supuesto como este, el Estado podría ser responsable por omisión, como consecuencia de no haber observado la debida diligencia[570].

En primer lugar, será necesario atender al propio concepto de terrorismo, pues este, también, ha sufrido una evolución en los últimos tiempos, como consecuencia de la adopción de criterios, que responden a cuestiones de oportunidad y no, de legalidad. Es decir, en determinadas ocasiones, la

---

equivalent of a classic (internationalized) non-international armed conflict, as was the case in Afghanistan from 19 June 2002 onwards, on which date a transition government was established. With the support of the international coalition, the newly established authorities were to deal with high-intensity fighting against organized nongovernment troops, i.e. those of the Taliban". VITÉ, S., *Typology of armed conflicts in international humanitarian law: legal concepts and actual Situations*. International Review of the Red Cross, vol. 91, no. 873. March 2009; pp. 69-94, en particular, p. 93.

568 Asi lo recoge, entre otros, MORENO FERNANDEZ, A.G., *La atribución al Estado de responsabilidad internacional por los hechos ilícitos de los particulares e intentos de flexibilización*. Revista Electrónica de Estudios Internacionales. 2006; pp. 32 y 34. Disponible en el sitio web: www.reei.org/index.php/revista/num12/ articulos/atribucion-al-estado-responsabilidad-internacional-hechos-ilicitos-particulares-intentos-flexibilizacion. Fecha de consulta, junio de 2013.

569 PAULUS y VASHAKMADZE, entienden que esta necesidad ya quedó demostrada "*by the 2006 Lebanon war, in which Israel destroyed considerable areas of southern and central Lebanon by military means to ward off rocket attacks by the Shia Lebanon-based political and paramilitary organization, Hezbollah. It is also demonstrated by the 2009 conflict in Gaza, in which Israel launched an air and ground offensive against Hamas, the Palestinian militant Islamist organisation. Less obvious is the characterization of Georgia's conflict(s) with its breakaway provinces of South Ossetia and Abkhazia before the Georgian attack on Tskhinvali on 7 August 2008 and the intervention of Russian forces, or of the conflict in Kosovo before the NATO intervention on 24 March 1999*". PAULUS, A. and VASHAKMADZE, M., *Asymmetrical war and the notion of armed conflict: a tentative conceptualization.* International Review of the Red Cross, vol. 91, no. 873. March 2009; pp. 95-125, en particular, p. 111.

570 MORENO FERNANDEZ, A.G., *La atribución al Estado de responsabilidad internacional por los hechos ilícitos de los particulares e intentos de flexibilización*, op. cit; p. 36.

calificación de unos hechos como ataque terrorista, ha conllevado la negación de una Parte en el conflicto. En consecuencia, cuando la actuación violenta, realizada por parte de un grupo, que manifiesta su confrontación con el Estado, es calificada de actividad terrorista, se cercena la posibilidad de reconocer la existencia de un conflicto armado no internacional. En consecuencia, toda vez que ese conflicto es inexistente, la aplicabilidad del DIH no llega a plantease. Por lo tanto, el Estado sigue haciendo uso de las medidas que, en el ámbito del Derecho interno, estén previstas para combatir este tipo de delincuencia. En estos supuestos, por lo tanto, el terrorista no tendrá la condición de combatiente que otorga el DIH y, por ende, no le estará permitido el uso de la fuerza, para la consecución de sus objetivos, ni existirán tales objetivos militares legítimos. De este modo, se puede llegar a privar, a determinados grupos, de la posibilidad de defender militarmente ciertos objetivos que, contemplados a la luz del DIH, serían militares y, por lo tanto, legítimos[571].

En este punto, resulta imprescindible atender a la visión del asunto, aportada por el CICR, que defiende que, entre el régimen jurídico que regula el terrorismo y el DIH, aplicable a los conflictos armados, ha de seguir respetandose una línea divisoria. El CICR, además de las circunstancias que han quedado ya reseñadas, señala que, el principio de igualdad constituye otra de las divergencias, entre ambos regímenes jurídicos. Es decir, la aplicación del DIH, a las Partes en conflicto, garantiza una situación jurídica de igualdad, mientras que, por el contrario, en caso de terrorismo, esta igualdad es inexistente, pues el terrorista no se halla constreñido por las limitaciones del DIH[572].

Ello ha llevado, a algunos autores, a abogar por la aplicación del DIH, en el caso de conflictos asimétricos[573]. Sin embargo, la complejidad del conflicto y, en

571 Estas reflexiones pueden encontrarse en *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*. Informe resultante de la XXXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Documento preparado por el Comité Internacional de la Cruz Roja. Ginebra, octubre de 2015; p. 21.

572 Así lo expresa el documento *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, doc. cit.; p. 21.

573 El profesor SCHMITT aboga por esta aplicación, justificando que "*Each of the cited forms of asymmetry – technological, doctrinal, normative, participatory, and legal or moral standing – exerts measurable influence on the application of international humanitarian law*". SCHMITT, M., N. *Asymmetrical warfare and International Humanitarian Law*, op. cit.; p.7.

la actualidad, la existencia de nuevas modalidades de combate, impiden que dicha línea divisoria, entre ambos regímenes jurídicos, pueda ser tan nítida. El conflicto asimétrico plantea la aplicación del DIH, desde el momento en que dicha asimetría se constata, en diferentes ámbitos y, no sólo, en el de las capacidades militares. Antes bien, la actuación de grupos organizados, como agentes no estatales, en los conflictos amados ha planteado la necesidad de abordar la asimetría jurídica, "*when a state fights a non-state entity that does not fulfil the criteria of Article 1 of Protocol II, but instead consists of armed bands without any hierarchical command structure that ignore both domestic law and IHL altogether*[574]". La desigualdad y desproporción, entre ambas Partes del conflicto, por lo tanto, no queda limitada a los medios y métodos de combate, sino que se extiende a un ámbito, en el que la calificación de los actos, de una de ellas, condicionará el régimen jurídico, aplicable al conflicto que libren.

En este sentido, incluso el CICR, sosteniendo la necesidad de separar las situaciones y calificarlas, jurídicamente, de forma distinta, reconoce la existencia de situaciones en las que el deslinde no resulta posible. De este modo, se constatan zonas comunes entre ambos regímenes jurídicos, es decir, aquellos casos en que "*el DIH prohíbe los actos específicos de terrorismo cometidos en un conflicto armado*", así como los actos de violencia "*en cuanto crímenes de guerra, cuando se cometen contra civiles o bienes de carácter civil*[575]". No obstante, el CICR se muestra contrario a que los actos, que no están prohibidos por el DIH, sean calificados como terroristas, en el ámbito interno o internacional, puesto que, de esta manera, se califican así, actos que en realidad no son ilícitos en el ámbito del DIH y, en consecuencia, puede desalentarse "*en el cumplimiento del DIH a los grupos armados no estatales que son parte de un conflicto armado no internacional*[576]".

En consecuencia, e interés, que un Estado puede manifestar en una u otra calificación jurídica, puede condicionar la que, finalmente, sea otorgada y esta

574 PAULUS, A. and VASHAKMADZE, M., *Asymmetrical war and the notion of armed conflict: a tentative conceptualization*, op. cit.; p. 109.

575 Así lo expresa el CICR *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, doc. cit.; pp. 22-23.

576 En este sentido, el CICR afirma que "*las normativas jurídicas que regulan los conflictos armados y el terrorismo no deberían amalgamarse*"; *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, doc. cit.; p.23.

calificación puede terminar siendo muy distinta de la que, con sujeción a los criterios estrictamente legales, sea la más adecuada.

Toda vez que, la propia definición de terrorismo no resulta pacífica[577], parece oportuno atender a una serie de criterios que indiquen en qué supuestos existe un conflicto armado. Así, se ha propuesto que, el hecho de que un Estado combata el terrorismo, a través de sus fuerzas Armadas, ha de entenderse un signo de que nos encontramos ante un conflicto armado, al igual que la intensidad y grado de organización, de las Partes involucradas en las hostilidades[578]. No obstante, la calificación de dichas hostilidades, como conflicto armado y, la consiguiente aplicación del DIH, en ningún caso, dependerán del principio de reciprocidad.

La calificación de determinadas actuaciones, como actividad terrorista, puede conllevar, pues, una serie de consecuencias negativas. Sin embargo, la calificación de conductas terroristas como ataques armados, tampoco ha sido alentada por el CICR, que considera que no puede hablarse de una lucha global contra el terrorismo para, de este modo, entender que, cualquier terrorista, donde quiera que se encuentre, puede ser un objetivo militar legítimo. La cantidad y entidad de ataques terroristas que se producen en la actualidad, ha llegado a plantear la cuestión de si, en estos casos, nos encontramos ante conflicto armado, al que sea de aplicación el DIH y, si el DIH podría aplicarse, igualmente, al crimen organizado internacional[579].

La repetida complejidad de las situaciones, a las que ha de hacerse frente, obliga a tener en cuenta tantos factores que, prácticamente impide una respuesta jurídica homogénea, que resulte adecuada para todos ellos. La perspectiva, desde la que se afrontan estos fenómenos, es realmente divergente. Así, para algunos

---

577 PAULUS y VASHAKMADZE reconocen, asimismo que "*States cannot even agree on a definition of terrorism itself*", PAULUS, A. and VASHAKMADZE, M., *Asymmetrical war and the notion of armed conflict: a tentative conceptualization*, op. cit.; p. 116.

578 Estos criterios son propuestos por PAULUS y VASHAKMADZE, para determinar en qué casos resulta necesaria la aplicación del DIH, como consecuencia de un conflicto armado. PAULUS, A. and VASHAKMADZE, M., *Asymmetrical war and the notion of armed conflict: a tentative conceptualization*, op. cit.; p. 116.

579 VITÉ, S., *Typology of armed conflicts in international humanitarian law: legal concepts and actualSituations*, op. cit.; pp. 92-94.

autores, como VITÉ, "*Al Qaeda's way of operating probably excludes it from being defined as an armed group that could be classified as a party to a global non international armed conflict*", de manera que las células, a través de las que dicho grupo se estructura, "*do not meet the organization criterion for the existence of a non-international armed conflict within the meaning of humanitarian law*". Sin embargo, el propio autor pone de manifiesto que, la Corte Suprema de los Estados Unidos consideró, de aplicación, el artículo 3 común a los Convenios de Ginebra, que ya ha sido antes citado, a los miembros de Al Qaeda y a "*quienes fueran capturados en la lucha contra el terrorismo*[580]". Asimismo, el Gobierno de los Estados Unidos sostiene la tesis de que el conflicto con dicho grupo terrorista es "*of an international nature and bases its authority to detain alleged terrorists on the international 'laws of war'*[581]".

Pues bien, la aplicación del DIH a grupos armados, más allá de su propio territorio, entendiendo que se sigue una lucha de naturaleza global, que justifica la conceptuación de ataque armado, no resulta adecuada a juicio del CICR. Antes bien, el Comité sostiene que, ni en el caso de Al Qaeda, ni en el supuesto del llamado Estado Islámico, existen "*elementos suficientes para considerar que el "núcleo" de Al Qaeda* (y del Estado Islámico) *y los grupos asociados a la organización en otras partes del mundo constituyen una única parte en el sentido del DIH*[582]".

No obstante, la aplicación del DIH, a conflictos que se libran contra grupos no estatales en territorio extranjero, sigue siendo defendida por autores, que consideran que el criterio del paso de fronteras resulta determinante, a la hora de calificar un conflicto armado internacional[583].

---

580 VITÉ, S., *Typology of armed conflicts in international humanitarian law: legal concepts and actual Situations*, op. cit.; p. 93. Fallo de la Corte Suprema de los Estados Unidos, en cita recogida por el autor, Supreme Court of the United States, Hamdan v. Rumsfeld, 548 US 557 (2006); pp. 65–69.

581 PAULUS, A. and VASHAKMADZE, M., *Asymmetrical war and the notion of armed conflict: a tentative conceptualization,* op. cit.; p. 110.

582 *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, doc. cit.; p. 24.

583 PAULUS y VASHAKMADZE justifican tal aplicación al entender que "*armed conflicts between a state's armed forces and transnational armed groups operating in the territory of another state without the latter's consent could be treated as international armed conflict because of the cross-border component. In this case, the law of international armed conflict, with its detailed humanitarian guarantees, would be applicable*". PAULUS, A. and VASHAKMADZE, M., *Asymmetrical war and the notion of armed*

En los conflictos armados internacionales, la actividad ciberterrorista podrá producirse, con el objetivo de prestar apoyo a una de las Partes en conflicto. En esos casos, será necesario calificar, adecuadamente, dicha actividad, de modo que el autor del acto en cuestión reciba el estatuto de combatiente o bien, la aplicación de la legalidad interna e internacional, relativa a los terroristas.

La actividad terrorista en internet, que ya fue objeto de atención en la Primera Parte el presente trabajo, podrá revestir distintas manifestaciones externas, pero en cualquier, caso conviene adoptar una postura restrictiva, al de calificar las conductas que, a través de la red se manifiestan como terroristas, o apoyo a grupos de dicha índole. Es decir, tal y como se abogaba al examinar el concepto de ataque armado, cometido por medios cibernéticos, la adopción de un criterio restrictivo se presenta como la solución más oportuna en estos casos. En ambos supuestos, la legalidad internacional resulta escasa e inadaptada a la actualidad. Asimismo, la práctica de los Estados todavía no es abundante y la Jurisprudencia Internacional no ha tenido ocasión de pronunciarse. Todos estos elementos constituyen factores adversos, a la hora de proceder a la calificación jurídica y tratamiento de nuevas figuras comisivas. Por ello, es necesario compartir la postura que, al respecto defiende el CICR y, en consecuencia, negar la aplicación del DIH al terrorista, así como su naturaleza de combatiente, salvo en aquéllos casos que no ofrezcan ninguna duda. De este modo, a través de la aplicación de este criterio restrictivo, se evitará extender el tratamiento de conflicto armado internacional a conductas que realmente no tienen tal naturaleza.

En lo que aquí respecta, pues, la ejecución de actos terroristas a través de internet, como los que se han estudiado en el Capítulo precedente, conllevará la aplicación de la legalidad interna e internacional, sobre terrorismo. En definitiva, los ciberterroristas que las lleven a cabo, no tendrán, *per se,* la condición de combatientes sino de terroristas. En consecuencia, los hechos ilícitos cometidos por estos ciberterroristas, no podrán ser atribuidos al Estado.

---

conflict: a tentative conceptualization, op. cit.; p. 112.

Los actos hasta ahora vistos, caen dentro de la definición que ESPADA RAMOS ofrece de "agresión indirecta"[584], al igual que los cometidos por los llamados "ejércitos de voluntarios" y, sobre los que se va a tratar a continuación, en la especifica forma que los mismos pueden manifestar en el cibercombate. Se trata en todo caso, de la expresión de una serie de actuaciones que puede llegar al uso de la fuerza y, respecto de las que, compartiendo las palabras de la misma autora, "*las normas de la Carta de Naciones Unidas que regulan el uso de la fuerza en concreto de encuentran desfasadas, respecto a los hechos reales*"[585]. Ciertamente, como se viene defendiendo, la legalidad internacional precisa una interpretación que ofrezca una respuesta lo mas adecuada posible a estos nuevos fenómenos. Los llamados cibervoluntarios pueden considerarse, asimismo, incluidos en esta necesidad de definición.

4.2.2. La atribución del hecho ilícito cometido por individuos o grupos organizados.

Como se desprende del análisis de la conducta terrorista, en gran parte de los supuestos, el agente no estatal que la lleve a cabo, recibirá el tratamiento jurídico que corresponde al personal civil. Por ello resulta determinante, ahora, establecer cuáles van a ser las consecuencias jurídicas de dicho tratamiento, así como los requisitos que son exigidos, por el DIH convencional y consuetudinario, para otorgar la condición de combatiente y, por último, los supuestos en que dicho personal civil, puede perder tal estatuto.

La participación de agentes no estatales en conflictos armados internacionales o no internacionales se perfila como un hecho probable, si se tiene en cuenta las posibilidades de participación, que ofrece la red y, a las que ya se ha

584 Para ESPADA RAMOS, esta agresión indirecta comprende, entre otros, los cometidos actos por "*bandas armadas para actuar dentro del territorio de otros Estados, los llamados ejércitos devoluntarios, el apoyo militar dado a las facciones en rebelión, el terrorismo y la subversión, con la idea de reeplazar los sistemas sociales y políticos existentes en un Estado*". ESPADA RAMOS, M.L., Nuevas formas de uso de la fuerza y su compatibilidad con el derecho Internacional actual". Estudios de Derecho Internacional Publico y Privado. Homenaje al Profesor Luis Sela Sampil. Universidda de Oviedo. 1970; pp. 301 a 323, en particular, pp. 311- 312.

585 ESPADA RAMOS, M.L., *Nuevas formas de uso de la fuerza y su compatibilidad con el derecho Internacional actual*, op. cit.; p. 322.

hecho mención. Por otra parte, dicha participación ha sido comprobada, en la realización de los principelas ciberataques hasta ahora conocidos. Ya se ha expuesto la dificultad de atribución de los ataques, cometidos por particulares, en Estonia y en Georgia. Cabe aquí, asimismo, mencionar los originados, con motivo del conflicto entre Rusia y Ucrania, a los que más adelante se hará una referencia más detenida. Si bien es cierto que, como se viene afirmando, ninguno de ellos llegó a la intensidad ni gravedad suficientes, para ser considerados ataques armados, sin embargo, conviene tener presentes estos supuestos, de modo que, cuando se reproduzcan en un futuro, los criterios que sirvan para determinar la atribución, se encuentren establecidos, con mayor claridad, de lo que están en el presente.

En consecuencia, se trata de establecer los caracteres que permitan dirimir, en qué casos el personal civil actúa por cuenta del Estado, hasta el punto de que a éste pueda ser atribuido el hecho ilícito. En la tarea de deslindar dichos criterios, será necesario examinar el DIH convencional y Consuetudinario, la jurisprudencia Internacional aplicable al caso y la doctrina internacionalista.

Se hace preciso aquí retomar la definición de personal civil formulada de modo excluyente, antes citada y, también, la obligación de protección contenida en el artículo 3 común a los Convenios de Ginebra para entrar a examinar en que momento, los grupos organizados, no estatales, dejan de ser civiles. En este sentido, será determinante conocer si el personal integrante de dichos grupos, pertenece, o no, a ese grupo organizado combatiente, en un sentido jurídico, es decir, si realiza lo que se denomina "*función continua de combate*[586]". El modo de organización de estos grupos diferirá entre unos y otros, pero se han constatado casos en los que era visible una sólida organización. Así, WATTS recoge las palabras de la Jefe del Consejo Nacional de Seguridad de Georgia que, al respecto, expone la que, a su juicio, es la capacidad de operaciones informáticas de Rusia del siguiente modo:

586 MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit; pp.32 - 33.

> "At the top of the hierarchy are the "Soldiers": the professional planners, computer scientists, engineers, and other implementers, including the military itself. Next are what some call the "Mercenaries." These are criminal organizations paid to carry out certain elements of the attacks. In this case, there are strong signs implicating an outfit known as the Russian Business Network (RBN). And, finally, there are the "Volunteers." These are individuals with PC's [sic] who are recruited to carry out attacks. They are provided with access to all the necessary software tools, as well as to detailed instructions for carrying out the attacks. Agencies and ministries of governments, not organized as armed forces, employ civilians to plan, directly support, and employ data stream CNA capabilities in support of international armed conflict" [587].

Pues bien, al respecto, la citada Guía del CICR, para interpretar la noción de participación directa en hostilidades, establece que, la calidad de miembro de estos grupos no puede depender de "*una adscripción abstracta*[588]". Antes bien, ello depende de si la función continua que se asume corresponde a la que ejerce el grupo de manera colectiva, es decir, la "*conducción de las hostilidades en nombre de una parte no estatal en el conflicto*[589]". Esta es la llamada "*función continua de combate*", que constituye, pues, el criterio para determinar, si un individuo pertenece a un grupo armado organizado. Para ello, será necesario determinar si esa función continua de combate existe, por cuanto, acreditada dicha existencia, las consecuencias que, de ello se derivan, resultan de suma importancia. Si el agente no estatal, que interviene en el conflicto, no ejerce dicha función de combate tendrá la calificación de personal civil, con todos los efectos jurídicos, que de ello se derivan. Asi será, en primer lugar, exigible el cumplimiento de la obligación, concerniente a la otra parte en el conflcito, de proteger a dicho personal, como consecuencia de la aplicación del principio de distinción.

Son ejemplos del ejercicio de dicha función de combate, como se veia en el Capitulo precedente, el uso de uniformes, de signos distintivos o portar determinadas armas. Nuevamente, nos encontramos con situaciones que resultan improbables de comprobar en la ejecución de una actividad cibernética, pero, en

587 Así lo pone de manifiesto WATTS, S. *Combatant Status and Computer Network Attack.* Virginia Journal of International Law, vol.50, issue 2. 2010; pp. 392-447, en particular, pp.410-411.
588 MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p.33.
589 *Ibidem.*

cualquier caso, estos indicios parecen conducir a una exigencia de que el participante, de algún modo externo, reconozca su inclusión en el grupo y se identifique con el mismo. De este modo, la Guía entiende que la función de combate también puede ser expresada por un comportamiento concluyente, tal como el hecho de "*participar directamente y de forma reiterada en las hostilidades para apoyar a un grupo armado organizado en circunstancias que indican que esa conducta constituye una función continua y no una acción espontánea, esporádica o temporal*[590]". Esta circunstancia resulta de constatación más sencilla, aunque su acreditación requiera el transcurso de un lapso de tiempo razonable, pues del texto se concluye que no es suficiente una única acción, sino una reiteración de actos. Esta pauta puede resultar, ciertamente útil, en el ámbito en que nos encontramos, pues, ese comportamiento concluyente sí puede darse en la red, a través de actos, como la ejecución de DDoS.

Por otra parte, el Manual de Tallin, en este ámbito, ofrece una serie de criterios de atribución de la conducta que, desde un punto de vista jurídico, no revisten la relevancia suficiente, para ser tenidos como Normas de atribución. Antes bien, las conclusiones presentadas en la Norma 8, han de entenderse como una mera presunción, de forma que, a falta de atribución evidente, operan como fórmulas que permitan descartar la responsabilidad del Estado. Como ya se apuntaba al tratar de la comisión del hecho ilícito, la Norma 8 del referido Manual propone el criterio de que una ciberoperación, haya sido dirigida, utilizando la ciberinfraestructura de un Estado, no es suficiente prueba, para atribuir esa operación a dicho Estado. No parece, por lo tanto, que la espinosa cuestión de los criterios de atribución pueda ser resuelta, únicamente, a través de la aplicación de las presunciones, contenidas en el repetido Manual. Puede compartirse el criterio expuesto por sus autores, en el sentido de que, no siempre el uso de la ciberinfraestructura se realizará, con el consentimiento del Estado, del que depende la misma. Pero tambien habra que atender a la Norma número 5, citada por la Norma 8, que propone que el Estado no puede consentir, a sabiendas, la utilización de su ciberinfraestructura para la realización de actos

590 *Ibidem*; p.34.

adversos a los derechos de otros Estados. Por ello, parece superflua la enunciación de la Norma 8, pues poco aporta a la imprescindible labor, de sentar los criterios, que fijen los supuestos en que la actividad particular pude ser atribuida al Estado.

La Compilación de DIH consuetudinario, por su parte, aborda la cuestión, haciendo referencia a la responsabilidad del Estado, por las violaciones cometidas por personas o grupos, que actúan, de hecho, obedeciendo sus instrucciones o, bajo su dirección o control. Se impone aquí, traer de nuevo al análisis, las consideraciones que se realizaban, al tratar la comisión del hecho ilícito. De este modo, de conformidad con la Norma 149, también antes aludida, un Estado puede ser considerado responsable de los actos de personas o grupos, que no sean sus órganos ni estén facultados, en virtud del Derecho interno, a ejercer prerrogativas gubernamentales. La atribución al Estado del hecho ilícito cometido por los mismos se producirá, siempre que dichas personas o grupos actúen obedeciendo sus instrucciones o, bajo la dirección o control de ese Estado.

En consecuencia, será determinante precisar cuáles hayan de ser esas "*instrucciones*" y, qué grado de control es el que el Estado ha de ejercer, sobre dicha conducta, para que la misma sea directamente atribuida a aquel. La cuestión del grado de control que haya de ejercerse sobre los individuos o grupos, ha sido tratado desde antiguo, por la doctrina internacionalista, así como por la Jurisprudencia Internacional y, de nuevo, presenta el máximo interés en la actualidad. Con carácter frecuente, los ataques que se constatan, en determinados conflictos armados y, también, algunos de los que tienen lugar en tiempo de paz, despiertan serias sospechas en cuanto a su autoría final. Es decir, si bien, en apariencia son lanzados por particulares o grupos, también lo es que la presencia de determinados Estados parece estar clara; sin embargo, en estos casos, la atribución al Estado ha resultado sumamente difícil[591].

591 Dos de estos ejemplos los constituyen China y Siria que, en palabras de SCHMITT y VIHUL, han cometido los siguientes hechos: "*Illustrating this point with a recent example, the Mandiant report indicated that the Chinese PLA's Unit 61398 (also known as Comment Crew or APT1) acted with the full knowledge and cooperation of the Chinese government. Some have challenged this assertion, but so long as the victim states acted with reasonable certainty based on clear evidence that China is behind the operations, they would have been within the bounds of the law in responding through demands for cessation, claims of*

Tradicionalmente, han sido dos los criterios que la Jurisprudencia Internacional ha manejado, en relación a dicho grado de control. La CIJ, en el asunto *Nicaragua,* en 1986, entendió que los Estados Unidos deberían haber tenido "*el control efectivo*" de las operaciones militares o paramilitares, en el curso de las que se produjeron las violaciones, de tal modo que, únicamente así, podría considerarse que los Estados Unidos eran responsables, de las violaciones de las obligaciones de DIH cometidas por los contras en Nicaragua[592]. La Corte en este supuesto entendió que las actuaciones llevadas a cabo por la contra, podrían haberse realizado,

> "without the control of the United States. For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed[593]".

En consecuencia, la Corte apreció la imposibilidad de atribuir los hechos ilícitos, cometidos por la *contra,* violando el DIH, a los Estados Unidos y responsabilizó, únicamente, a los componentes de dicho movimiento de tales actos[594].

---

reparations, or countermeasures. The same analysis applies to Syria's most prominent hacker group, the Syrian Electronic Army. Although it insists that it operates independently of the Assad regime, there are indications to the contrary. Injured states would be entitled to respond against Syria itself if sufficiently reliable and substantive evidence emerged that the relationship with the regime met the thresholds described above". SCHMITT M. N. & VIHUL, L. *Proxy Wars in Cyberspace,* op. cit.; pp.66-67.

592 La Corte se pronunció del siguiente modo: "*The Court has taken the view (paragraph 110 above) that United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua*." Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 115.

593 Military and Paramilitary Activities in and against Nicaragua, doc. cit.; par.115.

594 El fallo de dicha Sentencia recoge, en su apartado 9), la siguiente declaración: "*Finds that the United States of America, by producing in 1983 a manual entitled Operaciones sicologicas en guerra de guerrillas, and disseminating it to contra forces, has encouraged the commission by them of acts contrary to general principles of humanitarian law ; but does not find a basis for concluding that any such acts which may have been committed are imputable to the United States of America as acts of the United States of America.*"

En este ámbito que aquí se aborda, resulta imprescindible hacer alusión al criterio de control que, décadas después, estableció la Sentencia en apelación en el asunto *Tadic,* en 1999. En este caso, el TPAY entendió que "*la medida del control que se exige del Estado varia*". En consecuencia, el Tribunal, sostuvo que,

> "In the case at issue, given that the Bosnian Serb armed forces constituted a "military organization", the control of the FRY authorities over these armed forces required by international law for considering the armed conflict to be international was overall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations. By contrast, international rules do not require that such control should extend to the issuance of specific orders or instructions relating to single military actions, whether or not such actions were contrary to international humanitarian law"[595]

No obstante, como el Comentario al Proyecto señala, se trata de dos cuestiones distintas, en el sentido de que el Tribunal trata de dirimir la responsabilidad penal individual, y no la responsabilidad de los Estados "*y la cuestión planteada en el asunto del que se trata no concernía a la responsabilidad sino a las normas aplicables de derecho internacional humanitario*". En cualquier caso, el Comentario al Proyecto, de forma evidente, aboga por la asunción de un criterio basado en cada caso, de modo que se analice en cada supuesto si el comportamiento individual ha sido, o no, controlado por el Estado y, en qué medida puede serle atribuido[596].

No parece que la adopción de uno u otro criterio pueda establecerse, con carácter general para todos los casos sino, en efecto, tomando, como referencia, las circunstancias concretas de cada caso. En el supuesto que nos ocupa, resulta evidente que, la mera traslación de criterios, a los supuestos de ataques cibernéticos expuestos, resulta insuficiente. Es decir, tanto el criterio del control absoluto, como el del control general presentan dificultades en su aplicación. En relación al control absoluto, exigido en la decisión de la Corte relativa al caso de

595 Prosecutor vs. Dusko Tadic, Case nº IT-94-I-A, ICTY Appeals Chamber, Judgement 15 july 1999; par. 145.
596 Comentario 5) al artículo 8 del Proyecto.

Nicaragua, parece evidente que, el ámbito cibernético no es el más idóneo, para el ejercicio de dicho control por el Estado o, al menos, para la comprobación posterior, de que dicho control ha existido. Ya ha sido expuesto cómo, en determinados supuestos, la presencia de otro Estado, pese a ser posible, no ha podido ser probada. Esta dificultad de atribución, debida, principalmente al uso de las medidas, que se veían en el epígrafe segundo de este Capítulo, ha llevado a algunos autores, a defender la adopción de otros criterios, de menos exigencia. Así, SHACKELFORD entiende que la adopción de este criterio de control estricto conllevaría que, la exigencia de responsabilidad al Estado, por el lanzamiento de ciberataques, únicamente, podría darse "*if their effective control could be proven beyond* any doubt". Este hecho, a juicio del autor, conllevaría la inefectividad del criterio y, por ende, una irresponsabilidad absoluta para aquéllos Estados que decidieran patrocinar los ciberataques[597].

Pues bien, a la vista de las dificultades que ofrece la acreditación de la prueba y la consiguiente atribución[598], parece que la adopción de un criterio de mayor laxitud pudiera resultar una solución idónea, en orden a responsabilizar a los Estados de los ilícitos cometidos por sus individuos o grupos. Sin embargo, la exigencia de responsabilidad internacional al Estado, por la comisión de un hecho ilícito no puede ser objeto de una formulación, que termine vaciando de contenido dicha figura. Es decir, en el presente trabajo, en múltiples ocasiones se ha hecho mención a la necesidad de formular los conceptos que han de manejarse, en orden a lograr una verdadera adaptación, a las nuevas circunstancias y modalidades comisivas del hecho ilícito. Sin embargo, la adopción de determinados criterios de atribución, que pretenden salvar las dificultades

---

597 Para SHACKELFORD, "*In a sophisticated global cyber attack, missing or corrupted data commands may be sufficient to disprove State control and defeat accountability. Without either new techniques such as the probabilistic tracing project mentioned in Part II, or very unsophisticated hackers, effective control would make State responsibility for cyber attacks virtually a non-starter.*" SHACKELFORD, S. J., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Conference on Cyber Conflict Proceedings 2010 C. Czosseck and K. Podins (Eds.) CCD COE Publications,2010,Tallinn,Estonia; p. 202.

598 STINISSEN explica cómo la dificultad de atribución fue constatada, asimismo, en los ataques sufridos por Ucrania y cómo la teoría de control efectivo no podría haberse aplicado: "*Snake, Blackenergy, and Sandworm reportedly have a Russian connection, actively supporting. Mere operational support does not meet the 'overall control' threshold*". STINISSEN, J., A., *Legal Framework for Cyber Operations in Ukraine*, op. cit.; pp. 123-134.

técnicas que aquí concurren, pudieran, asimismo, presentar desventajas desde un punto de vista práctico y también jurídico.

SHACKELFORD, en este sentido, recuerda que, cuando el individuo o grupo actua por cuenta del Estado, el hecho ilícito puede ser atribuido a dicho Estado, en aquéllos supuestos en que el Estado no observe la diligencia debida. En estos casos, el autor entiende que, la responsabilidad por omisión puede atribuirse siguiendo el creiterio sostenido por la CIJ en el fallo del caso de la embajada de los Estados Unidos en Teheran, de 1980[599]. Dicho autor, tomando como base esta Sentencia, defiende la extensión del criterio a los ciberataques, en los supuestos en que los ciudadanos de un Estado actúen por cuenta de un órgano de gobierno de un Estado y, también, en los supuestos de ausencia de prueba suficiente, adoptando el criterio del conocimiento gubernamental[600].

Sin embargo, no puede compartirse plenamente el planteamiento defendido por el autor porque, un criterio excesivamente laxo podría suponer la atribución de un hecho ilícito, a un Estado que, en realidad, no ha tenido ninguna participación. Nuevamente, hay que recordar las específicas técnicas que permiten el anonimato y el enmascaramiento de la identidad en internet y que, éstas podrán utilizarse para crear la falsa apariencia de que, un Estado se encuentra patrocinando los ciberataques de un grupo[601].

---

599 El apartado 3) del fallo de la Sentencia, emitida por la CIJ, establece la obligación de poner fin a la violación de la obligación internacional. El fallo, al respecto, cita las obligaciones internacionales violadas por Irán, al establecer que la CIJ "*3)"Decides that the Government of the Islamic Republic of Iran must immediately take al1 steps to redress the situation resulting from the events of 4 November 1979 and what followed from these events, and to that end : (a) must immediately terminate the unlawful detention of the United States Chargé d'affaires and other diplomatic and consular staff and other United States nationals now held hostage in Iran, and must immediately release each and every one and entrust them to the protecting Power (Article 45 of the 1961 Vienna Convention on Diplomatic Relations). (...)*". United States Diplomatic and Consular Staff in Tehran, doc. cit; fallo, par. 3.

600 El autor aboga por la adopción de este criterio, en los siguientes términos: "*This reasoning could be extended to cyber attacks in two ways. First, the standard could be adopted that, if the citizens of a State acted on behalf of a competent government organ, then the government could be vicariously liable for the resulting damage from such cyber attacks. Second, if there is insufficient evidence to find attribution outright, as there was in Iran hostage, then the standard could become one of governmental awareness, i.e. if the government was aware of its obligations under international law to prevent its citizens and information infrastructure from launching cyber attacks and failed to comply with these responsibilities*". SHACKELFORD, S. J., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, op. cit.; p. 203.

601 Al hablar del enmascaramiento de la identidad militar, de los equipos y sistemas, PADMANABHAN, advierte de la posibilidad de que ello llegue a producirse. En consecuencia, estas técnicas, de aplicación probable en el combate, deberán ser tenidas en cuenta, asimismo,

En consecuencia, la atribución que no se base en un control efectivo, por parte del Estado, sin que haya lugar a dudas, puede resultar errónea y, por lo tanto injusta. Una atribución del hecho ilícito, realizada en ausencia de estas exigencias, podría dar lugar a exigir la responsabilidad internacional de un Estado que, en realidad, ha sido víctima de un ataque, al haberse fingido su identidad.

En efecto, el criterio del control general podría adoptarse, con carácter prioritario, respecto del criterio del control efectivo y, de este modo, podrían haberse atribuido determinados ciberataques que se han producido recientemente[602].

En la adopción de ambos criterios habrá que dirimir, con carácter previo, hasta qué punto el personal civil que, voluntariamente, se involucra, en el desarrollo de ciberoperaciones durante un conflicto armado, pertenece, o no, a una de las Partes en conflicto. En función de esa pertenencia o, en ausencia de ella, a dicho personal le corresponderá la condición jurídica de legítimos beligerantes o, por el contrario, nos encontramos ante civiles, cuyo estatuto de no combatiente ha de ser respetado. En consecuencia, perderán dicha protección como personal civil en tanto participen en las acciones propias del combate. Parece, en este punto, recomendable seguir la indicación, antes apuntada, por el Comentario de artículos del Proyecto pues, en efecto, los modos y grados de participación y, el tipo de control, por parte del Estado, admiten una casuística, ciertamente, numerosa. Tampoco puede olvidarse aquí, la trascendencia que dicho control puede tener, en orden a la calificación misma del conflicto armado, como internacional o no internacional. Los ataques cibernéticos sufridos por

---

para delimitar, con certeza, los criterios de atribución. Al respecto el autor, señala que"*cyber warriors (…) are also likely to hide the military nature of computers used in a cyber operation by employing the outward markings of civilian computer infrastructure, such as a civilian Internet Protocol (IP) address*". PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*, op. cit.; p. 295.

602Así SHACKELFORD entiende que: "*For example, if the overall control standard were used instead of effective control, it would be possible that Russian or Chinese incitement behind the cyber attacks on Estonia, Georgia, or the United States, if proven, would be sufficient to satisfy State attribution. But if effective control remains the dominant paradigm for determining State responsibility for cyber attacks, even a victim State of a worst-case scenario cyber attack may not receive justice*". SHACKELFORD, S. J., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, op. cit.; p. 204.

Ucrania durante el conflicto con Rusia, son una muestra reciente de dicha circunstancia[603].

Por otra parte, hemos de recordar, nuevamente, que nos encontramos con un elemento, el cibernético, que, como repetidamente se ha señalado, puede estar al alcance de una gran parte de la población y que puede ofrecer grandes ventajas, a quienes hagan uso del mismo. Por lo tanto, la participación de civiles en los conflictos armados, a través de internet, parece una tendencia que, lejos de desaparecer es probable que se propague en el futuro.

En determinadas ocasiones, esa actuación no tendrá más trascendencia que la de expresar el apoyo a una de las Partes en conflicto, sin que, los hechos cometidos, tengan relevancia, desde el punto de vista del DIH[604]. Así, los llamados hacktivistas a los que se hacía referencia en el Capítulo precedente, no realizan actividades que puedan considerarse un ataque armado, ni que lleguen a revestir entidad suficiente, para que ellos sean considerados personal beligerante. En estos casos, como afirma PADMANABHAN, la falta de relación de estos individuos con el Estado impide cualquier atribución de su conducta a aquél y, en consecuencia "*Such a loose affiliation with the State is unlikely to meet the standard for "belonging to a Party" to the conflict because hacktivists are not under the "effective control" of the State*[605]."

Pues bien, incluso, asumiendo que, el establecimiento del control del Estado, necesario para la atribución de las conductas particulares, ha de hacerse de forma individualizada y según las circunstancias de cada caso, sin embargo, es preciso establecer unas referencias mínimas, que permitan abordar dicha labor con garantías. En consecuencia, es necesario acudir al concepto de la

603 STINISSEN, en este sentido, apunta: "*The International Committee of the Red Cross (ICRC) has characterised the situation in eastern Ukraine as a 'non-international armed conflict. If Russia actively participates or exercises 'overall control' over the separatists, the conflict could be considered an international armed conflict. To meet the criterion of 'overall control', a state must not only finance, train, equip, or provide operational support to local forces, but also have a role in*". STINISSEN, J., A *Legal Framework for Cyber Operations in Ukraine*, op. cit.; pp.123-134.

604 Este es el caso de los miembros de Al Qaeda, que como recoge PADMANABHAN "*have admitted to engaging in "low-level and disruptive" cyber operations including sabotage of political websites and denial of service attacks as part of their organization's war with the United States*". PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello* , op. cit.; p. 296.

605 *Ibidem*.

participación directa en hostilidades, en orden a determinar, en qué casos el personal civil, realmente, se halla vinculado a la Parte contendiente y, en definitiva, al Estado[606]. En este sentido, la Guía entiende que para que haya una relación, de facto, entre el individuo que combate y el Estado, han de darse indefectiblemente tres requisitos: una declaración formal, un acuerdo tácito o un comportamiento decisivo[607]. En cualquiera de los tres supuestos, la conducta del individuo será atribuible al Estado, porque se entenderá que el individuo combate por cuenta del Estado. Sin embargo, será difícil probar alguno de dichos requisitos, si no hay una voluntad expresa del individuo. En cualquier caso, como se ponía de manifiesto anteriormente, puede concluirse que la Guía exige una actuación que resulte concluyente y que, por lo tanto, propone un criterio restrictivo, que ha de compartirse.

Por otra parte, el mismo documento exige que la actuación del personal civil sea claramente manifestada, ademas de, capaz de causar un daño de suficiente gravedad y que se realice con la intención de ayudar a una Parte beligerante. Estos tres requisitos, pues, habrán de ser analizados, caso por caso, para determinar si, en efecto, los cibervoluntarios actúan por cuenta del Estado.

La participación de los civiles en el conflicto armado, de manera individual o formando parte de un grupo organizado, puede revestir muy diversas modalidades y expresarse en distinto grado. Así, volviendo a la interpretación conceptual que ofrece la Guía, hay que analizar la definición de participación en hostilidades que es recogida como "*la implicación de una persona en esas hostilidades*", entendidas éstas, a su vez, como el "*recurso por las partes en conflicto a medios y métodos de causar daño al enemigo*[608]" y que podrá manifestarse de forma directa o indirecta. Asimismo, se hace mención a las hostilidades como la "*totalidad de los actos hostiles realizados por las personas que participan directamente*

606 Esta cuestión ha sido puesta de manifiesto asimismo por parte de la OTAN en los siguientes términos: "*Cyber is a highly specialised area in which the armed forces of NATO member countries employ civilian specialists or outsource tasks. The notion "direct participation in hostilities*". PITERS, H. *Cyber Warfare and the Concept of Direct Participation in Hostilities*. NATO Legal Gazette. Legal issues related to cyber, issue 35. December 2014; pp.46-57, en particular, p. 47.
607 MELZER, N., S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p.23
608 *Ibidem*; p.43.

en las hostilidades". Nuevamente, la Guía aboga por una interpretación restrictiva al entender que "*de conformidad con el DIH la interpretación del concepto de participación directa en las hostilidades debe limitarse a actos hostiles específicos*", es decir aquéllos ejecutados por personas como parte de la conducción de las hostilidades entre partes en un conflicto, tanto internacional como no internacional[609]. La aplicación de un estatuto de combatiente o la consideración de civiles a quienes son cibervoluntarios, tuvo relevancia, asimismo, en el caso de los ataques sufridos por Ucrania[610].

Por otra parte, del examen que el CICR realiza en la citada Guía, se extraen tres elementos que habrán de estar presentes para poder afirmar la participación directa en las hostilidades[611]: que dicha participación alcance el umbral del daño, que constituya una causa directa del mismo, que exista un nexo beligerante y que todo ello se de en un espacio temporal determinado.

Pues bien, si por daño, comúnmente, se entiende la producción de una lesión física, el deterioro, la destrucción de un bien o, incluso, la muerte, en ese punto el CICR, amplia el concepto de daño a la producción de "*cualquier consecuencia adversa en las operaciones militares o la capacidad militar de una parte en conflicto*[612]".

Pues bien, si asumimos que la producción de un daño, cuando se trata de operaciones cibernéticas, puede consistir en cualquiera de las actuaciones enumeradas en el texto que se examina (una interferencia electrónica en las redes

---

609 *Ibidem*; p.45.

610 Asi lo expresa STINISSEN al referirse a los mismos en el siguiente sentido: "*For example, the defacement of websites and DDoS attacks restricting the use of internet services violated Ukrainian criminal law and could have been prosecuted in Ukrainian courts. During the occupation of Crimea and the armed conflict in eastern Ukraine, the Law of Armed Conflict applies. It regulates the conduct of all actors in the conflict, including the cyber actors. Most cyber actors in Crimea were nominally non-state actors, for example the pro-Russian hacker group CyberBerkut*". STINISSEN, J., *A Legal Framework for Cyber Operations in Ukraine*, op. cit.; pp.123-134.

611 La Guia interpretativa publicada por el CICR, en su Capitulo V, aborda la definicion de estos requisitos. MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; pp.46-64.

612Además, ofrece un ejemplo especifico, en relación a las operaciones cibernéticas al manifestar que en este contexto "*podría bastar una interferencia electrónica en las redes informáticas militares, sea mediante ataques a la red informática o la explotación de la red informática, así como la interceptación de las líneas telefónicas de los altos mandos de la parte adversaria o la transmisión de información o inteligencia táctica en relación con los objetivos de un ataque*". MELZER, N., S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p. 47.

informáticas militares, sea mediante ataques a la red informática o la explotación de la red informática, así como la interceptación de las líneas telefónicas de los altos mandos de la parte adversaria o la transmisión de información o inteligencia táctica en relación con los objetivos de un ataque), cabría pensar que, en este ámbito se abandona el criterio restrictivo que, hasta ahora, parecía imponerse.

Sin embargo, tal conclusión no puede alcanzarse por cuanto, la exigencia del resto de los requisitos impedirá una ampliación del concepto de participación en hostilidades cuando se trate de ciberoperaciones. Aquí, parece que las indicaciones de la Guía pretenden abarcar la producción de daños, que no tiene una manifestación estrictamente física. De este modo, cabe concluir que la mera *interferencia* tendrá que suponer la producción de un daño porque, de otro modo, se estaría supeditando la comprobación del hecho, al éxito de la operación o ataque. Es decir, si para la constatación de la participación directa en las hostilidades, se exigiera la producción de un daño físico, como consecuencia del ataque, quedaría desvirtuada la aplicación de estos criterios, a las operaciones cibernéticas, pues dicha producción no siempre tendrá lugar ni será, en todos los casos, el resultado perseguido. Ya se ha visto como, la mera *interferencia*, tuvo efectos muy negativos, en la gestión de determinados servicios, cuando los ataques se produjeron en Estonia. Por el mismo motivo, ha de extenderse la aplicación de este criterio, a los supuestos en los que dichos ciberataques se produzcan, durante el desarrollo de un conflicto armado.

Asimismo, parece conveniente considerar que los actos, que no tienen efectos adversos, sobre las operaciones o la capacidad militar de una parte en conflicto, constituirán participación directa en las hostilidades, cuando sea probable que "*el acto específico cause como mínimo, la muerte heridas o destrucción*[613]". En el supuesto citado anteriormente, de los ataques sufridos por Ucrania, esta consideración vuelve a cobrar relevancia, pues como se ha señalado, "*In the case of*

613 MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit; p. 49.

CyberBerkut and other active hacker groups the effects probably did not reach the threshold of harm"[614].

Sin embargo, cuando la Guía retoma el supuesto de los ataques informáticos, especifica parece tener presentes las vulnerabilidades de las infraestructuras criticas, en los termino que aquí se han expuesto previamente, porque el texto advierte que, "*la manipulación de redes informáticas (…) pueden tener un grave impacto en la seguridad pública, la salud y el comercio y es posible que estén prohibidos según el DIH*[615]". No obstante, aun teniendo presente tal realidad, el CICR no extiende el concepto de causación de daño suficiente, a los ataques informáticos que no causen efectos militares adversos. Es decir que, en el lanzamiento de los ciberataques, la comprobación de la participación directa en hostilidades, dependerá de la causación de dicho daño, concretado en los efectos militares adversos, que ya han sido antes señalados; criterio, que ha sido juzgado como excesivamente restrictivo por algunos autores[616]. En este sentido, cabe remitirse a las valoraciones, antes realizadas, en torno al papel que, las empresas gestoras de infraestructuras criticas, pueden llegar a desempeñar en el conflicto, sobre las que no procede ahora volver.

En relación al criterio apuntado por el CIRC y, aun cuando parte de la doctrina lo considere mas restrictivo, de lo deseable, ha de tenerse por un criterio acertado. Las consideraciones apuntadas son coherentes con la minoracion que la Cruz Roja pretende conseguir, en relación con la participación de civiles en el conflicto armado y que se ha puesto ya de relieve en los diversos documentos que se han ido citando. Por otra parte, hay que celebrar la adopción de tesis

614 STINISSEN, J., *A Legal Framework for Cyber Operations in Ukraine*; p. 132.

615 MELZER, N., S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p. 50.

616 PADMANABHAN entiende que "*By contrast, those exploiting civilian systems for the purpose of harming the economic prospects of an enemy State would likely not meet the threshold of harm, unless they destroy civilian infrastructure in the process of doing so. Michael Schmitt has criticized the threshold of harm standard for being "under-inclusive" in terms of the conduct included within the ambit of direct participation. Schmitt questions why the Interpretive Guidance limits participation to acts that cause "death, injury, or destruction" to civilians and civilian property, as opposed to including any harmful acts directed against protected persons and objects that are part of war strategy or are evidently related to ongoing hostilities. Application of the threshold of harm standard to cyber warriors demonstrates the strength of these concerns*". PADMANABHAN, V., M., *Cyber Warriors and the Jus in Bello*, op. cit.: p. 299.

cautelosas, en este ámbito, ante la pretendida extensión de conceptos a circunstancias facticas que no reunen las características exigidas por los primeros. Pese a que, a lo largo del presente estudio, se ha reiterado la necesidad de interpretar la legalidad internacional, para dar cabida a fenómenos novedosos, como el que aquí se trata, ello no puede utilizarse para justificar la desvirtuacion de los mismos o la acreditación de beligerantes y de conflictos bélicos en situaciones que, estrictamente, no lo son.

En segundo lugar, como se ha anticipado, la participación directa en las hostilidades exige que ésta constituya una causalidad directa, en los actos del conflicto armado. Es decir, que dichas actividades se distingan, de aquellas que constituyen una "*parte del esfuerzo general de guerra o que pueden caracterizarse como actividades en apoyo de la guerra*[617]". La mera intervención, en apoyo de una de las Partes, pues, no puede ser entendida como una participación directa en el conflicto. Habrá que tener aquí presente entonces, que no toda actividad constituye un ataque o participación y, como aclara STINISSEN, «*cyber operations are very often called "cyber attack". "Attacks" means acts of violence against the adversary, whether in offence or in defence. Not every cyber operation that affects the adversary is an attack*[618]».

Las muestras de solidaridad o apoyo que, por internet, pudieran recabarse, respecto de los objetivos perseguidos, por uno de los contendientes, no será tenido por participación, en el sentido aquí expresado. Ello es sumamente relevante por cuanto, de nuevo, este criterio tiene que ser apreciado, a la hora de discernir entre actividades terroristas y, aquéllas que constituyen actos de guerra. Como se ponía de manifiesto en el epígrafe precedente, la aplicación del DIH a los miembros de grupos terroristas presentes en un conflicto o que, pudieran desencadenarlo, no parece aconsejable habida cuenta el riesgo de alterar la naturaleza jurídica del concepto de conflicto armado. La adopción de un criterio restrictivo en este punto, coopera, nuevamente, en la misión de mantener una postura como la anteriormente expresada.

617 MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p. 51.
618 STINISSEN, J., A *Legal Framework for Cyber Operations in Ukraine,* op. cit.; p. 132.

Por otra parte, teniendo en cuenta que la presencia de ciberactivistas en los conflictos armados será, previsiblemente, cada vez más frecuente, conviene excluir del concepto de combatientes, de forma expresa, a determinados grupos cuya actividad no presenta una relevancia suficiente. La Guía ejemplifica la ayuda que pueden prestar quienes manifiesten su apoyo a uno de los contendientes, en actividades políticas, económicas, o en apoyo al esfuerzo general, a través de los medios de comunicación, ejerciendo labores de propaganda o transacciones financieras[619]. Pues bien, ya se ha visto cómo, estas actividades son realizadas, de manera frecuente, por los grupos terroristas, en apoyo a su propia causa o bien, como sostenimiento a los objetivos militares de conflictos en curso[620].

Por último, hay que tener presente que dicha actividad, que ha de constituir la causa del daño, ha de ser "*bastante próxima entre el acto y el consiguiente daño*" y, por ende, la causalidad directa ha de entenderse de manera que, el daño en cuestión se produzca, por "*una sola secuencia causal*[621]". Es decir, como SCHMITT y VIHUL resumen, "*merely encouraging or generally supporting non-state actors' cyber operations does not qualify, nor does having the ability to somehow influence the non-state actor's actions*"[622]. La proximidad causal implica que el empleo de medios y el daño han de ser directos, con independencia, de la proximidad temporal o geográfica del atacante. Este criterio favorecerá, en el ámbito que nos ocupa, la atribución del hecho ilícito, en el sentido de que, precisamente, el lanzamiento de ciberataques o ciberoperaciones se hará en con cierta distancia temporal y geográfica, sin que ello impida atribuir la autoría de

619MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p. 51.

620 Asimismo, PADMANABHAN pone de manifiesto cómo este criterio también ha se ser útil para distinguir entre combatientes y meros activistas en la red: "*The requirement of "belligerent nexus", In the context of cyber warriors the requirement would distinguish between patriotic hacktivists objectively seeking to aid their country in war and groups like Anonymous55 that may commit very similar attacks but with no intention to benefit belligerents*". PADMANABHAN, V. M, *Cyber Warriors and the Jus in Bello*, op. cit.; 299.

621 MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p. 53.

622 SCHMITT, M., N. & VIHUL, L., *Proxy Wars in Cyberspace*, op. cit.; p.64.

los mismos, a diferencia de otros métodos de combate, que requerirán cierta inmediatez para el logro de un resultado mínimamente exitoso.

Nuevamente, los ciberataques que se produjeron durante el conflicto armado entre Ucrania y Rusia, constituyeron una prueba más, de la naturaleza no beligerante de los ataques lanzados, por individuos, de forma particular. Es decir, la exigencia de este nexo beligerante determina la exclusión del concepto de participación directa, en hostilidades, de todos aquéllos, cuya actividad, *a priori,* pudiera suscitar sospechas, pero cuya relevancia en el desarrollo del combate es, en definitiva, mínima. Así, como expresa STINISSEN, la principal actividad durante el citado conflicto, consistió en "*information warfare and intelligence gathering – not to damage cyber or critical infrastructure*[623]."

El nexo beligerante no puede hacerse depender del ánimo de cada uno de los participantes, puesto que, "*muchas actividades durante un conflicto armado carecen de un nexo beligerante, aunque causen una cantidad considerable de daño*[624]". Es decir, en coherencia con lo hasta ahora expuesto, a lo largo del desarrollo del conflicto, podrán originarse una diversidad de actuaciones, que no constituyan una participación directa en las hostilidades, como la comisión de ciberdelitos o, de actos de terrorismo, a través de internet. Pues bien, aun cuando estas actividades causen danos no constituyen una participación directa de esos individuos en las hostilidades y, por lo tanto, no pueden ser atribuidos a ningún Estado.

Por último, la participación en las hostilidades, indefectiblemente, irá unida a un criterio temporal. De forma coherente con lo dispuesto en el DIH convencional, la participación directa en las hostilidades requerirá la comprobación, coetánea, a la calificación jurídica del estatuto del individuo o grupo que participa. De acuerdo con el PA I, el personal civil sólo será objetivo militar durante el tiempo en que se produzca dicha participación[625]. Como ya se

623 STINISSEN, J., A *Legal Framework for Cyber Operations in Ukraine*, op. cit.; p. 132.

624 MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit; pp. 59- 60.

625 Textualmente, el articulo 51 del PA I, en su apartado 3, afirma que "*Las personas civiles gozarán de la protección que confiere esta Sección, salvo si participan directamente en las hostilidades y mientras dure tal participación*".

exponía, al hablar de la vigencia de la obligación violada, el criterio temporal, en el ámbito cibernético también requiere una interpretación, adecuada a la naturaleza del mismo pues, el momento en que se produzca la comprobación de los efectos de un ataque informático o, incluso, su propia producción, puede distar en el tiempo de aquél en que el mismo ataque se produjo[626].

Este ámbito temporal cobra una especial relevancia puesto que "*Los miembros de grupos armados organizados que pertenecen a una parte no estatal en un conflicto cesan de ser civiles mientras mantengan esa calidad de miembros en virtud de su función continua de combate*[627]". En consecuencia, deberán ser tenidos por combatientes. Esta calificación implicara una serie de obligaciones, para quienes se hallan en tal situación pero, correlativamente, también las tendrá, para la otra Parte contendiente. Como, reiteradamente se ha manifestado, a ambas partes en el combate les compete la obligación de distinguir entre objetivos militares y personas o bienes civiles que gozan de tal protección.

Esta obligación motiva la necesidad de establecer una serie de pautas, que faciliten la distinción, entre el personal civil y el combatiente, durante el conflicto, incluso, cuando la actividad de los particulares se realice a través de la red. Presumiblemente estas situaciones no se manifestaran de forma clara pues, como se ha visto, las modalidades de participación en el conflicto son variadas y, por lo tanto, será necesario acudir, nuevamente, a los criterios interpretativos que ofrece la Guía. Cabe resaltar, en este punto que, en los casos en que pueda existir alguna duda al respecto, el CICR defiende presumir la condición civil del participante, entendiendo que la conducta del particular o grupo, "*no llega a ser una participación directa en las hostilidades*"[628]. Sin embargo, como el propio documento advierte, esto no impedirá el uso de la fuerza necesario, por parte del Estado, para el mantenimiento del orden público. En el ámbito de los ataques

626 Así lo advierte también PADMANABHAN, "*Iran, for example, was not aware that the problems with its centrifuges were related to foreign sabotage until well into the Olympic Games program.57 Strict interpretation of the "such time" language could well insulate civilians involved in pro-grams like Olympic Games from targeting by States*" . PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*, op. cit.; p. 300.

627 MELZER, N. S., Interpretive Guidance on the notion of direct participation in hostilities, op. cit.; p. 70.

628 *Ibidem*, p. 70.

cibernéticos, las actuaciones de apoyo al conflicto armado, podrán revestir formas delictivas o terroristas, como ya se ha mencionado y, en consecuencia, originar la aplicación del derecho interno.

Una cuestión que, en este ámbito, puede tener, incluso, más relevancia que en el combate convencional, es la relativa a la cuestión de lo que ha venido a denominarse, "*revolving door*". Es decir, las "puertas giratorias", a las que determinado personal civil puede acogerse de forma tal que, en un momento dado, sea combatiente e, instantes después, deje de serlo, para pasar a tener, de nuevo, protección como personal civil. Si en el combate convencional, esta cuestion ha planteado problemas, en la participación en las hostilidades a través de internet, se aventura como un inconveniente de gran dimensión, habida cuenta la facilidad que este medio ofrece para intercambiar las funciones que se realizan.

En el caso de los cibervoluntarios, la acreditacion de los elementos requeridos para su consideración como combatientes o, participantes en las hostilidades, presenta, igualmente, una dificultad interpretativa. La prueba de que, el grupo conduce las hostilidades de una Parte o, con el acuerdo de una de las Partes beligerantes, será de difícil obtencion. Por este motivo, conviene recordar que, precisamente, la dificultad de atribución de la autoría será uno de los mayores alicientes que los Estados podrán encontrar a la ahora de encargar el lanzamiento de ciberataques o ciberoperaciones a los particulares, con el objetivo de evitar su responsabilidad internacional.

Por otra parte, la necesidad de que el combatiente se muestre uniformado, en el desarrollo del conflicto, plantea la cuestión de, qué ha de entenderse por uniforme en el ámbito digital. Para PADMANABHAN[629] consistirá en el uso de una IP militar, que permita identificar al atacante como usuario de un equipo informático militar. Ciertamente, parece que la uniformidad, entendida como el distintivo que, en el mundo físico, permite la identificación de las Partes de un conflicto, debería tener su equivalente virtual en el IP. Sin embargo, no pueden olvidarse ahora, las consideraciones que ya se han hecho, en epígrafes

629 PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*, op. cit.; p. 295.

precedentes, en torno a la posibilidad de ocultar esa IP y, aun de atribuirlo, de forma engañosa. Por lo tanto, el hecho de que esa IP, desde la que, aparentemente, se lanzan los ataques u operaciones sea militar podría tenerse en cuenta, a mero título de presunción. De obstante, de la misma manera que los autores del Manual de Tallin proponen que la utilización de la infraestructura cibernética de un Estado, puede tomasre como indicio para una posterior atribución, la identificación de una IP podrá considerarse un indicio de la posible autoría. En consecuencia, las mismas reticencias que se exponían en torno a la primera de las propuestas han de manifestarse en cuanto a la realizada por el autor citado.

Sin embargo, sí puede concluirse con el autor que "*a requirement that in order to be a lawful combatant a cyber warrior must use a military IP address in his attacks incentivizes transparency in cyber operations. Transparency mitigates the risk*[630]".

En esta tarea de deslinde de los supuetsos concretos en que podrá darse la participación civil en las hostilidades, a través de la red, hay que traer d enuevo a estudio, los casos más relevantes, constatados hasta la fecha. Cabe recordar que ni en el caso de Estonia ni en el de Georgia, los ciberataques verificados, alcanzaron la entidad suficiente como para ser tenidos por tales, de conformidad con el concepto de ataque armado que ha sido expuesto. En el más reciente caso de Ucrania, idéntica conclusión se alcanza. Como pone de manifeisto STINISSEN "*Most of the cyber activities in Ukraine however are information operations and do not meet the 'attack' threshold*". [631] Sin embargo, el hecho de que la doctrina internacionalista califique, jurídicamente, estas actuaciones como operaciones de información y, no como o ataques armados, no supone un impedimento, a la hora de analizar las cuestiones de atribución. En contraposición a lo que el autor antes citado expone, las operaciones de información pertenecen al desarrollo del combate y, por lo tanto, deben respetar el DIH. En consecuencia, la transgresión del DIH, en una operación de esta índole, podría suponer la comisión de un

630 *Ibidem*.
631 STINISSEN, J., *A Legal Framework for Cyber Operations in Ukraine*, op. cit.; p.133.

hecho ilícito. Por lo tanto, también, en ese caso, nos encontraríamos ante la necesidad de abordar su atribución.

Asimismo, el autor califica las actuaciones relacionadas, con la obtención de datos e información y considera que las mismas forman parte de la actividad de ciberespionje. Hay que afirmar que, en efecto, aquí no cabe la aplicación del DIH, salvo en las circunstancias que en el epígrafe correspondiente se han visto. De la misma manera que se exponía la inconveniencia de aplicar el DIH a los ciberterroristas, con el objetivo de evitar una innecesaria expansión de los conflictos armados, aquí debe abogarse por la misma tesis restrictiva.

Los ataques que, hasta ahora, han sido objeto de estudio por la doctrina internacionalista, han demostrado el posible potencial y protagonismo que, otros ciberataques análogos, pudieran tener en un futuro. Sin embargo, ninguno de ellos ha revestido una gravedad que permita encuadrarlos, jurídicamente, en el concepto de ataque armado. Asimismo, la participación en las hostilidades, por parte de sus autores, no parece estar completamente clara, si aplicamos los criterios aportados por la Guía. No obstante, como se ha advertido, la posible acreditación de ciberataques armados en el futuro o la participación directa en hostilidades de cibervoluntarios, justifican la atención a cuestiones como las que aquí se analizan, en relación a la atribución al Estado de esos ilícitos. En casos como los aquí vistos, también habrá que optar por una solución restrictiva. De esta forma, puede sostenerse que, únicamente, en el caso de que los cibercombatientes actúen por cuenta de una Parte beligerante, podra atribuirse el hecho ilícito a ese Estado.

La actuación a través de la red requiere de una mayor exigencia, a la hora de acreditar los requisitos que se han expuesto, pues como se viene demostrando, la confusión, que el propio entorno permite, en cuanto a la autoría, requiere mayor precisión en su atribución. Sería necesario, por lo tanto, que los cibervoluntarios actuaran de forma organizada, a favor de los intereses militares de una de las Partes beligerantes y que dicha parte, de una u otra forma, manifestara su conformidad con dicha actuación o, en su defecto, pudiera probarse un vínculo entre el Estado y los voluntarios, como el suministro de

equipos, software o conocimientos o el favorecimiento de su ocultación. Únicamente, al concurrir unos elementos como los descritos, podría alcanzarse una mínima seguridad sobre la autoría y sobre la atribución del hecho, al Estado favorecido por la actuación.

Resta, finalmente, por analizar un último criterio de atribución al Estado del hecho ilícito cometido por los particulares, previsto en el artículo 11 del Proyecto, cuyo tenor literal determina que

> "El comportamiento que no sea atribuible al Estado en virtud de los artículos precedentes se considerará, no obstante, hecho de ese Estado según el derecho internacional en el caso y en la medida en que el Estado reconozca y adopte ese comportamiento como propio".

Del texto transcrito se desprende que la conducta, que no es atribuible a un Estado, en aplicación de los artículos precedentes, todavía puede ser considerada un acto atribuible al Estado, por el Derecho Internacional, si el mismo conoce y adopta, como propia, la conducta ilicita.

Este supuesto previsto por el Proyecto podría darse en el caso de que, a pesar de no haberse podido probar la autoría de determinados ciberataques, el Estado los hubiera reivindicado como propios. No parece, sin embargo, una circunstancia de probable concurrencia en el futuro. De lo expuesto hasta ahora se concluye que, al contrario, internet puede ser utilizado por los Estados, para eludir la responsabilidad internacional exigible por su transgresión de las normas de DIH y el hecho de que, una vez producido el ciberataque, éste sea asumido por el Estado, no parece que vaya a producirse con facilidad.

No obstante, también aqui, cabe plantearse qué criterios habrá que tener en cuenta, en los supuestos de hechos ilícitos, cometidos a través de internet, al objeto de disponer de unas mínimas pautas, cuando la situación se presente en el futuro.

La interpretación de la expresión "*reconocer y adoptar*" un hecho "*como propio*", en el caso de un ciberataque, no debería ofrecer más complejidad, que en el caso de que el hecho ilícito se hubiera cometido, por otros métodos de combate. Sin embargo, hay una circunstancia, concurrente en todos los casos que, hasta

ahora, se han constatado, y es la ventaja o beneficio obtenido por un Estado, a través de la actuación de ciber voluntarios en el conflicto. Es decir, en los casos de Estonia, Georgia y Ucrania parece evidente que Rusia obtuvo cierta ventaja, de la actuación de quienes lanzaron los ciberataques que aquí se han señalado. Al menos, quedó, en su día, reforzada su posición en los distintos conflictos, a través, del apoyo recibido con dichas actuaciones, en la red. Sin embargo, desde el estricto análisis fáctico, ninguna asunción de autoría se produjo por parte de Rusia. Ello originó la imposibilidad de exigir responsabilidad internacional a ningún Estado y aun de someter a la justicia interna a determinados sujetos identificados como responsables [632] . Igualmente paradigmático resultó el supuesto del virus Stuxnet, aunque en este último caso sí parece que ha existido algún tipo de asunción de autoría, sin que, evidentemente, la misma alcance la entidad suficiente, para encuadrarla en el supuesto de este artículo 11 que aqui se analiza[633].

Por lo tanto, a la vista del comportamiento observado por los Estados, con posterioridad a los hechos referidos, no resulta ocioso plantearse el alcance de los conceptos, presentes en el artículo 11 del Proyecto. Para los autores del Manual de Tallin el reconocimiento y la aceptación han de estar simultáneamente presentes y, además, manifestarse de forma expresa[634]. También el Comentario al Proyecto de artículos entiende que ambas condiciones son acumulativas, aunque admite que las mismas no sean expresas, sino que se deduzcan del comportamiento del Estado[635].

---

632 En relación con las consecuencias de los ciberataques producidos en Estonia, Lituania y Georgia, nos remitimos a la obra señalada anteriormente, TIKK, E. KASKA, K., RÜNNIMERI, K., KERT, M., TALIHÄRM, A.-M., VIHUL, L. Cyber Attacks Against Georgia: Legal Lessons Identified. En relación con los incidentes acreditados en Ucrania puede consultarse STINISSEN, J., *A Legal Framework for Cyber Operations in Ukraine*.

633 Asimismo, los hechos relacionados con el virus Stuxnet y la falta de acreditación de su autoría, ha sido citada a lo largo del presente trabajo, entre otros en los siguientes documentos: ZIOLOWSKI, K. *Stuxnet-Legal considerations*, op. cit; LIN, H., *Cyber conflict and international humanitarian law*, op. cit.; pp.515-531 y WAXMAN, M. C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* op. cit.; pp.421-459.

634 No solo son las condiciones de conocimiento y adopción acumulativas sino que, además, requieren algo más que una mera aprobación o asunción tácita. SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; pp.29-34.

635 Comentario 9) al artículo 11 del Proyecto.

El reconocimiento y aceptación tendrán consecuencias de carácter absoluto, pues tal y como pone de manifiesto la Compilación de DIH Consuetudinario, en el momento en que ésos se producen, el hecho ilícito pasa a ser un hecho del Estado, "*independientemente del hecho de que la persona o entidad involucrada no fuese, en el momento de la comisión de los actos, un órgano del Estado ni se le hubiera encargado la comisión de los mismos en nombre del Estado*[636]" y así lo refleja la práctica de los Estados.

En este orden de cosas es importante tener presente, de nuevo, la escasa práctica de los Estados, acreditada hasta la fecha, toda vez que ningún Estado ha reconocido, ni aceptado los ataques constatados. Para que ello se hubiera producido parece aceptable exigir un reconocimiento formal y expreso que, de forma indubitada, señale al Estado en cuestión, como autor del ciberataque. En su defecto, como afirma el Comentario al Proyecto, bastaría un comportamiento del que se deduzca tal atribución, que debería ser tan concluyente, que permitiera asimilarlo con un reconocimiento expreso. En consecuencia, el hecho de que un Estado muestre sus simpatías o apoyo a los ciberataques, que se lanzan por un grupo de voluntarios o un Estado que no niegue su implicación en los ataques que, desde determinados sectores de la opinión pública se imputa, no puede entenderse como un comportamiento, del que se induzca la atribución de un hecho ilícito[637]. Bien es cierto que las acusaciones reiteradas contra un Estado, que no son negadas por éste podría originar confusión, pero este elemento no es suficiente, para atribuir un hecho ilícito a un Estado. En este sentido, parece conveniente tener en cuenta los criterios, que han sido aplicados por la Jurisprudencia para entender asumida una conducta, por parte de un Estado. En el caso de los rehenes estadounidenses retenidos en la Embajada de Teherán, la CIJ sostuvo que el hecho ilícito, no había sido cometido activamente por parte del

636 HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; pp. 606-621.

637 También para SCHMITT y VIHUL el reconocimiento ha de ir más allá de un mero apoyo, "*Thus, for example, if a state expresses approval for particular non-state cyber operations against another state and subsequently acts to support them, as in mounting cyber defences to foster their continuance, the acts become attributable. However, this is a relatively limited basis for attribution. Merely expressing support or encouraging the non-state actors is insufficient*". SCHMITT, M. N.& VIHUL L., *Proxy Wars in Cyberspace*, op. cit.; p. 64.

Estado de Irán, porque no había intervenido ninguno de sus agentes estatales. Sin embargo, la Corte considero que la conducta posterior resultó, de tal forma esclarecedora en ese sentido, que debía declarase responsable internacionalmente, al Estado por lo ocurrido. El Tribunal, en la Sentencia relativa al caso expreso esta argumentación en el siguiente sentido:

> "The policy thus announced by the Ayatollah Khomeini, of maintaining the occupation of the Embassy and the detention of its inmates as hostages for the purpose of exerting pressure on the United States Government was complied with by other Iranian authorities and endorsed by them repeatedly in statements made in vanous contexts. The result of that policy was fundamentally to transform the legal nature of the situation created by the occupation of the Embassy and the detention of its diplomatic and consular staff as hostages. The approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible. On 6 May 1980, the Minister for Foreign Affairs, Mr. Ghotbzadeh, is reported to have said in a television interview that the occupation of the United States Embassy had been "done by Our nation". Moreover, in the prevailing circumstances the situation of the hostages was aggravated by the fact that their detention by the militants did not even offer the normal guarantees which might have been afforded by police and security forces subject to the discipline and the control of official superiors"[638].

Es decir, la asunción de un hecho ilícito, a posteriori, por parte de un Estado exige una conducta activa, sin que sea suficiente, pues, una pasividad persistente, aun cuando ésta resultara incompatible, con el esclarecimiento de los hechos o pudiera llegar a generar confusión. De la misma manera, no parece lógico que el Estado al que se le pretende atribuir un hecho ilícito, se encuentre en la necesidad de negar acusaciones que no revisten ningún fundamento.

La atribución del hecho ilícito, en estos supuestos, tendrá que ser, por lo tanto, indubitada, sin que las dificultades técnicas, que aquí se han venido manifestando, hayan de favorecer la adopción de criterios laxos, que mermen la

638 United States Diplomatic and Consular Staff in Tehran, doc. cit.; par. 74.

seguridad jurídica internacional. Tampoco en este caso, puede abandonarse el criterio restrictivo, cuya defensa se ha ido manteniendo a lo largo del presente trabajo, pues se presenta como el más eficaz en la tarea del cumplimiento de la legalidad internacional.

5. CONCLUSIONES AL CAPÍTULO TERCERO.

Cuando un ciberataque constituya un método de combate prohibido por el DIH, surge la necesidad de que el mismo sea atribuido a un Estado, pues de otro modo, la exigencia de responsabilidad internacional será inviable. La comisión cibernética del hecho ilícito y la participación de diversos agentes estatales y no estatales en el conflicto armado origina una serie de cuestiones de las que se extraen las siguientes conclusiones:

PRIMERA: La atribución al Estado de un hecho ilícito implica una dificultad adicional, en la indagación de la autoría, cuando el ilícito sea cometido a través de un ciberataque armado. La ocultación de la autoría resulta inherente al uso de la red, pero cuando los Estados y los agentes no estatales entran en la red, a través de NAT, proxies o redes TOR, se añade una dificultad adicional en la acreditación de esa autoría, que no existe en la utilización de otros métodos de combate. Sin embargo, puesto que la presencia en redes ocultas no es exclusiva de los agentes no estatales, sino que también puede darse en los Estados, este acceso debería permitir una mejor indagación del hecho ilícito. Estas oportunidades deberían hacerse valer por los Estados, de forma que su acceso al internet oculto fuera utilizado para lograr identificar a quienes se ocultan en él.

SEGUNDA: Un ciberataque armado, contrario al DIH, cometido por los miembros de las Fuerzas Armadas en el combate, será atribuido al Estado en la práctica totalidad de las ocasiones en que se produzca. El uso de los ciberataques como método de combate por parte de los miembros de las Fuerzas Armadas permitirá su atribución al Estado de un modo que podrá decirse casi automático.

En este caso, la doctrina general expuesta en el Proyecto de artículos no solo no encuentra ningún obstáculo en su aplicación, sino que se ve favorecida al atender a estos agentes del Estado, pues los métodos de combate estarán siempre a disposición de las Fuerzas Armadas. La obligación de los miembros de las Fuerzas Armadas de condicionar el uso de este método de combate a la legalidad internacional implica que cualquier desviación, respecto de la legalidad internacional, constituirá un hecho ilícito atribuible al Estado.

De nuevo es necesario poner de relieve que existe una obligación genérica de respetar el DIH, que se encuentra presente en los cuatro Convenios de Ginebra y que puede ser infringida tanto por acción como por omisión. En consecuencia, el Estado será responsable de la contravención del DIH por la actuación de sus Fuerzas Armadas, tanto por acción como por omisión.

La atribución al Estado de los hechos cometidos por los miembros de sus Fuerzas Armadas parte de un criterio de tal amplitud que, incluso, en los supuestos en que un miembro de las Fuerzas Armadas cometa el hecho ilícito, sin intención de hacerlo, ese hecho ilícito será atribuible al Estado. Este criterio amplio no puede abandonarse, pues favorece el cumplimiento de la legalidad internacional. La especial naturaleza del método de combate cibernético implica una mayor exigencia en la diligencia que han de observar los combatientes. Una disminución en el control de la actuación de los miembros de las Fuerzas Armadas podría tener como consecuencia un incremento de la comisión de los hechos ilícitos. Por otra parte, si el criterio de atribución se restringiera, como debe ocurrir cuando el hecho ilícito es cometido por agentes no estatales, podría originar un incumplimiento sistemático de las limitaciones impuestas por el DIH. En consecuencia, la novedad y complejidad que supone el empleo de este método de combate deberá ser acompañada de un adiestramiento adecuado.

En numerosas ocasiones, se ha puesto de relieve la necesidad de que los miembros de las Fuerzas Armadas tengan un conocimiento preciso de las normas de DIH. En este caso, esa necesidad es especialmente exigible al Estado. Únicamente desde un conocimiento preciso de los límites que el DIH impone a

los ciberataques utilizados como método de combate, podrá evitarse la comisión de hechos ilícitos y su consiguiente atribución al Estado.

Esta formación específica no podrá limitarse a quienes se encuentren encargados de la dirección de las ciberoperaciones, sino que, en distinta medida, deberá ofrecerse a todo el personal militar. En relación con los primeros, la prohibición de los ciberataques que se trataba en el Capítulo anterior deberá quedar expuesta de forma clara y específica. Es decir, las sesiones de formación y adiestramiento que se ofrezca a quienes se hallen encuadrados en las Secciones o Mandos encargados de ciberdefensa deberán advertir del hecho de que los ciberataques son un método de combate y que el mismo ha de utilizarse cuando exista una necesidad militar, respetando la distinción entre objetivos civiles y militares, sin causar daños innecesarios o desproporcionados, sin incurrir en perfidia y respetando la neutralidad de terceros. Esta formación específica debería ofrecerse de forma periódica y, con mayor énfasis, en el momento previo al despliegue. Los Contingentes que vayan a participar en Operaciones de Mantenimiento o imposición de la Paz, bajo mandato de las Naciones Unidas o al amparo de la OTAN o de la UE, deberán contar con dicha formación. Por lo tanto, la fase de concentración previa al despliegue en la que se da a los miembros del Contingente la información precisa sobre la operación que se va a desarrollar, parece un momento oportuno para reflejar estas cuestiones. En relación al específico personal, encargado de las ciberoperaciones, deberá tenerse en cuenta la distinta responsabilidad que desempeñen en la cadena de Mando. Como resultado, debería ofrecerse una información adecuada a cada uno de ellos, que comprendiera el contenido del Anexo de ciberdefensa que contenga el Plan de Operaciones y de las Reglas de Enfrentamiento de ciberdefensa que pudieran aparecer en el catálogo de ROE´s aplicables a la operación.

Aun cuando este adiestramiento es esencial, no puede considerarse único, pues, como se adelantaba, la formación en el ámbito de ciberseguridad tendrá que estar al alcance de todo el personal del Contingente. Si en otros aspectos de las operaciones militares esto no parece tan necesario, aquí se justifica, por la disponibilidad que gran parte del personal puede tener de equipos o sistemas

que permiten la comisión de un ilícito cibernético. Además, la formación adecuada evitará la atribución al estado de los hechos ilícitos que se cometan por omisión.

Cuando se utilice un método de combate prohibido, el hecho ilícito que se produzca se atribuirá al Estado, como consecuencia de la omisión del debido control. Así se refleja en las disposiciones del Proyecto y de sus Comentarios, sin que exista ninguna razón para que, en el caso de los ciberataques en el combate, esta doctrina quede sin aplicación. El Estado será responsable, por lo tanto, de los hechos cometidos por sus agentes, es decir, los miembros de las Fuerzas Armadas, por negligencia o, incluso, por error. En todo caso, el criterio determinante será que dicha comisión se realice en uso de las atribuciones conferidas o bajo la apariencia de autoridad.

Incluso, en los supuestos en que el hecho ilícito se cometa desoyendo las órdenes del Mando o con extralimitación en el cumplimiento de las mismas, será atribuido al Estado si, su autor ha tenido acceso a medios oficiales. Aun cuando pudiera parecer que la aplicación de estas presunciones supone la adopción de un criterio excesivamente amplio, en realidad, nos encontramos ante una situación que requiere este tratamiento. En el desarrollo de las Operaciones se dará la presencia de un personal habilitado para el manejo de determinado armamento y material que, de otro modo, no estaría a su alcance y el correcto uso del mismo es responsabilidad, en última instancia, del Estado. La atribución, pues, de los actos *ultra vires* se producirá cuando el agente estatal se exceda de sus cometidos asignados, con independencia de cuál sea la orden recibida.

Esta atribución al Estado, planteada de un modo que podría decirse general o prácticamente global, encuentra su única excepción en los supuestos en que la conducta no haya sido autorizada por el Mando militar ni éste haya podido ejercer control sobre quien lanza la operación o ataque cibernéticos.

TERCERA: La ayuda o asistencia de otro Estado en un ciberataque armado, prohibido por el DIH, han de acreditarse en virtud de un criterio restrictivo. La complejidad de las actuaciones en la red conllevará,

previsiblemente, la actuación conjunta de varios Estados para conseguir el ciberataque o ciberoperación. Cuando se constate la cooperación de otro Estado, por ejemplo, permitiendo el uso de redes o la venta de armamento cibernético, será exigible la responsabilidad del Estado que presta ayuda o asistencia en virtud de lo dispuesto en el artículo 16 del Proyecto.

Sin embargo, la restrictividad que se defendía para acreditar la existencia de un ciberataque armado ha de ponerse de manifiesto nuevamente ahora. Precisamente la habitualidad en esta cooperación entre los Estados, tiene que incidir de forma directa en la consideración de la misma desde una perspectiva prudente. También en este aspecto, tiene que recordarse la naturaleza de arma de doble uso que concurre en internet. Ésta, igualmente, redundará en una actividad comercial entre los Estados que puede dificultar la atribución en los supuestos de uso ilícito. Si partiéramos de la base de que cualquier actuación entre los Estados ha de tenerse por cooperación en el hecho ilícito podríamos encontrarnos con la atribución del mismo a un Estado cooperante que ha vendido equipos, sistemas o programas, desconociendo la utilización ilícita de la que iban a ser objeto. Por lo tanto, los criterios que establece el proyecto de artículos en orden a determinar la cooperación o asistencia al Estado infractor han de ser respetados y, además, interpretados con cautela.

De este modo, el Estado que ha realizado la transacción anteriormente apuntada o que permite el uso de su ciberinfraestructura a un tercero deberá tener conocimiento de las circunstancias en que dichos elementos están siendo utilizados por el Estado infractor. Este conocimiento debe ser equiparable a la complicidad, porque, de otro modo, se atribuirá el hecho ilícito a un Estado que no ha gozado de una mínima capacidad de control.

Además, la entidad de la ayuda o asistencia que se preste tendrá que ser determinante. En consecuencia, se tendrá que acreditar la realización de un hecho ilícito, por parte del Estado que presta tal ayuda o asistencia, que podrá consistir, por ejemplo, en proporcionar al Estado infractor un arma cibernética o en financiar su desarrollo. En los casos de transferencia de armamento, el Estado que suministra el arma cibernética será responsable de las violaciones de las

obligaciones de DIH si conoce que el Estado receptor comete violaciones sistemáticas del DIH.

Para la acreditación de estos extremos será imprescindible acudir a la información con la que cuente el primer Estado, obtenida a través de sus canales oficiales, entre los que habrá que contar el ciberespionaje. Asimismo, en este sentido, serán especialmente útiles los programas destinados a compartir información entre los entes públicos y privados y entre Estados.

Por último, la obligación de no prestar ayuda o asistencia también tiene que entenderse como una consecuencia de la obligación que tienen los terceros Estados de hacer respetar las normas de DIH. En consecuencia, al Estado que presta ayuda o asistencia, en el sentido expuesto, se le podrá atribuir el hecho ilícito y, además, será responsable de la violación de esta obligación internacional.

CUARTA: La atribución al Estado de los ciberataques prohibidos por el DIH, producidos por agentes no estatales en el conflicto armado, impone la adopción de un criterio restrictivo.

La actuación de agentes no estatales en el conflicto implica la adopción de una premisa restrictiva, que no puede verse modificada por la necesidad urgente de dar respuesta a las nuevas circunstancias del conflicto armado.

En efecto, la presencia de agentes no estatales en el conflicto puede verse incrementada, precisamente, como consecuencia de las ventajas que ofrece el uso de la red. Ya se ha mencionado, al hilo de distintas reflexiones, cómo la asimetría del conflicto es una característica que se presenta, cada vez más, en la conducción de hostilidades. La participación de individuos, ciberterrorristas y cibervoluntarios ha sido ya constatada y, con toda seguridad, no se tratará de un fenómeno efímero, sino con tendencia a incrementarse.

Por ese motivo, es necesario que la atribución al Estado del hecho ilícito cometido por estos agentes no estatales cuente con unas pautas de identificación que resulten claras y también estrictas. De nuevo se pone en evidencia la necesidad de contar con un concepto de ciberataque armado que permita descartar todas aquellas actividades manifestadas a través de la red que eran

excluidas de este concepto en el capítulo previo. En los modernos conflictos armados, serán frecuentes los ataques informáticos que se produzcan tanto en apoyo como en contra de cualquiera de las Partes en el conflicto. Sin embargo, en escasas ocasiones alcanzarán la entidad suficiente para tenerlas por un ciberataque armado y, quedarán, por lo tanto, sometidas a la legalidad que les es propia y que ya se expuso.

No obstante, en los casos en que dichos cibervoluntarios realmente incidan en el conflicto armado a través de ciberataques armados, habrá que delimitar en qué supuestos el mismo es atribuible a un Estado. Nuevamente, nos encontramos con la extraordinaria dificultad en la indagación de la autoría apuntada en la primera de estas conclusiones. Sin embargo, ello no puede justificar la defensa de determinados criterios interpretativos, que parecen más dirigidos a ofrecer una respuesta práctica que a abogar por la que sea conforme con la legalidad internacional. En el caso de los llamados cibervoluntarios, el criterio determinante para atribuir el hecho ilícito a un Estado será el de la participación directa en las hostilidades. De la misma manera que este criterio ha servido para considerar combatientes a quienes participen directamente en las hostilidades, utilizando cualquier otro método de combate, deberá ahora tenerse en cuenta, cuando el método de combate sea el cibernético.

El hecho de que internet sea un arma de doble uso vuelve a poner de manifiesto la disponibilidad de la misma por una gran parte de agentes no estatales y esta disponibilidad se ha traducido, en la práctica, en la posibilidad real de participar en el conflicto armado. La acreditación de esa participación constituye el paso previo a la atribución del hecho ilícito al Estado y se dará cuando reúna una serie de requisitos.

En el ámbito del cibercombate, la participación de cibervoluntarios en el conflicto se considerará una participación en las hostilidades, si el ataque informático constituye un acto hostil específico que tenga la suficiente capacidad como para afectar negativamente a las operaciones militares o a la capacidad militar de una de las Partes en el conflicto armado. Con base en esta apreciación, han de descartarse, pues, todos los supuestos de hacktivismo, ciberdelincuencia e,

incluso, ciberterrorismo que se exponían en el capítulo precedente, aunque también estén presentes en el conflicto. La necesidad de que el ciberataque constituya un acto hostil, vuelve a conducir las cuestiones de atribución hacia el concepto restringido de ciberataque armado. Además, esta participación debe guardar relación directa con el daño producido y ser idónea para producirlo. Es decir, que cuando se produzca una actuación por parte de cibervoluntarios, en un conflicto armado, ésta ha de revestir, prácticamente, los mismos caracteres que las que desarrollen las Fuerzas Armadas, al menos, desde un punto de vista fáctico.

La tesis restrictiva que ahora se defiende viene avalada, además, por el hecho de que, una vez constatada esa participación directa, la misma tiene que ser atribuible al Estado. Y ello sólo ocurrirá cuando el ciberataque hostil sea producido por un agente no estatal, sobre el que el Estado ejerza tal control que sus actos han de entenderse cometidos por el propio Estado. Se trata, por lo tanto, de mantener en este aspecto, una postura coherente con lo establecido por la Jurisprudencia internacional, que entiende no es suficiente un mero conocimiento de los hechos por parte del Estado para atribuir el hecho ilícito, sino que es necesario probar la existencia de ese control.

Las doctrinas jurisprudenciales, en relación al control estricto de los actos de grupos organizados, por parte del Estado, no pueden entenderse superadas por criterios menos exigentes, sino por una tesis que permita la adaptación del criterio a la concreta casuística. Y, en consecuencia, los ciberataques contrarios al DIH, que se cometan en el conflicto armado por agentes no estatales, sólo podrán ser atribuidos al Estado cuando éste se encuentre realmente ejerciendo el control sobre dichos agentes.

Nuevamente, la novedad del método de combate y la dificultad adicional en la indagación de la autoría no pueden conducir a la propuesta de soluciones que desvirtúen la legalidad internacional ni a las que, a buen seguro, debilitarían la seguridad jurídica internacional.

Este criterio, con el que pretende defenderse el respeto a la legalidad internacional, ha de mantenerse con todas sus consecuencias, incluso asumiendo que, en algunos casos, será inviable la atribución del hecho ilícito al Estado.

PARTE II

LAS CIRCUNSTANCIAS O CAUSAS QUE EXCLUYEN LA ILICITUD DEL CIBERATAQUE UTILIZADO COMO MÉTODO DE COMBATE

CAPÍTULO CUARTO. LA NATURALEZA IMPERATIVA DE LAS NORMAS DE DIH QUE CALIFICARÍAN A UN CIBERATAQUE COMO UN MÉTODO DE COMBATE PROHIBIDO.

1. INTRODUCCIÓN.

Si la obligación responsabilidad internacional es, por si misma, una nueva relación jurídica surgida del hecho [639], es decir, de la violación, por acción u omisión de una obligación internacional por medio de un ciberataque utilizado como medio de combate, corresponde ahora examinar las posibles causas de exclusión de responsabilidad internacional que podrían ser alegadas por el Estado autor del referido ciberataque para eximirse de la obligación de responder internacionalmente.

En el Proyecto de artículos se dedica su Capítulo V a las circunstancias que excluyen la ilicitud de un comportamiento que, de otro modo, sería calificado como ilícito, por cuanto no es conforme con las obligaciones contraídas por dicho Estado. En concreto, se recogen seis circunstancias o causas que excluyen la ilicitud: el consentimiento; las contramedidas; la fuerza mayor; el peligro extremo y el estado de necesidad (artículos 20 a 25 del Proyecto, respectivamente). En consecuencia, al concurrir alguna de estas circunstancias, como señala la CDI en sus comentarios al Proyecto, "constituye una defensa contra una reclamación por el incumplimiento de una obligación internacional, que, de mediar esa defensa, estaría bien fundada"[640]

Sin embargo, esta regla general está condicionada por la excepción contenida en el artículo 26 del Proyecto de artículos, en el que se establece que: "*Ninguna disposición del presente capítulo excluirá la ilicitud de cualquier hecho de un Estado que no esté en conformidad con una obligación que emana de una norma imperativa de derecho internacional general*". Atendiendo a que las obligaciones internacionales que pueden ser violadas, a través de un ciberataque utilizado

639 PEREZ GONZALEZ, M. *La responsabilidad internacional (II)*, en Instituciones de Derecho Internacional Público, Diez de Velasco, M. Tecnos. Madrid 2013; p. 872.
640 Comentarios al Proyecto de artículos.

como método de combate, pueden tener la naturaleza de norma imperativa de derecho internacional general o norma de *ius cogens,* resulta necesario dirigir nuestros esfuerzos, en una primera instancia, a las cuestiones relativas a las normas imperativas.

La atención a las normas imperativas de derecho internacional general o normas de *ius cogens* ofrece un nuevo punto de dificultad en la labor investigadora desarrollada hasta el momento, por cuanto que constituye una cuestión jurídica controvertida en sí misma, al no estar bien delimitados sus límites y efectos jurídicos. Como consecuencia, la polémica doctrinal respecto al *ius cogens* internacional no ha dejado de proliferar, hasta el punto de que la propia existencia de normas imperativas de derecho internacional general ha sido cuestionada.

El proceso de codificación y desarrollo progresivo del Derecho Internacional nos ha ofrecido luz en relación con la propia existencia del *ius cogens,* especialmente a través de la encomiable labor desarrollada por la CDI. Así lo podemos comprobar con la inclusión de las normas imperativas en el ámbito del Derecho de los Tratados (artículos 53 y 64 de la Convención de Viena de 1969). Será en el artículo 53 del referido Convenio donde se constate la existencia de normas imperativas de derecho internacional general o de *ius cogens*, al establecer que:

> *"(…)* Para los efectos de la presente Convención, una norma imperativa de derecho internacional general es una norma aceptada y reconocida por la comunidad internacional de Estados en su conjunto como norma que no admite acuerdo en contrario y que sólo puede ser modificada por una norma ulterior de derecho internacional general que tenga el mismo carácter" [641].

Con la inclusión de esta clara definición de las normas imperativas, al atender las causas de nulidad absoluta de los tratados internacionales, se deja sin sentido a las distintas corrientes doctrinales que han puesto en duda su

641 Convenio de Viena sobre el Derecho de los Tratados, de 23 de mayo de 1969.

existencia[642]. Sin embargo, aun no compartiendo los postulados negacionistas, es de rigor dejar constancia de las corrientes doctrinales que justifican la ignorancia de tales normas. Así, cierto sector de la doctrina entiende que no hay consenso en Derecho Internacional en relación al contenido normativo del concepto[643].

No obstante, como se señala en el Informe Anual de la CDI de 2014, "si bien en la actualidad el reconocimiento del *jus cogens* como parte de la estructura moderna del derecho internacional apenas suscita controversias"[644], siguen siendo objeto de polémica otras cuestiones sustantivas como son su naturaleza, la determinación de qué normas podrían ser consideradas como normas de *ius cogens,* así como sus consecuencias en el ámbito jurídico internacional. Así, aun por quienes admiten su existencia, existe polémica en torno a esas cuestiones sustantivas, como tendremos ocasión de apuntar, como, por ejemplo, con una errónea identificación de las normas imperativas con las normas *erga omnes,* aun cuando las primeras surtan efectos *erga omnes.* Sin embargo, casi lo más llamativo es que aún se requiera, en la actualidad aclarar que el *jus cogens* forma parte del ordenamiento jurídico internacional. En este sentido se manifestaría la CDI en su Primer Informe sobre el *Ius Cogens:* "(…) Si bien […] el número de quienes cuestionan el concepto viene disminuyendo con rapidez, todavía es necesario aclarar que el *jus congens* está firmemente establecido como parte del derecho internacional vigente"[645]. En este Primer Informe, además, se deja constancia de cómo el *ius cogens* ha sido objeto de recepción por parte de la Jurisprudencia internacional, desde la aprobación de la Convención de Viena sobre el Derecho

642 En este sentido, puede atenderse a la recopilación de corrientes doctrinales contrarias al reconocimiento del ius cogens que realiza VEDROSS, en VEDROSS, A. *Jus dispositivum and Jus cogens in International Law.* American Journal of International Law. Vol. 60, 1966; pp. 55 a 63.

643 LINDERFALK se expresa en los siguientes términos: "*Sceptics accept the rules enshrined in the Vienna Convention concerning the effects of jus cogens, emphasizing, however, that in international law consensus has not (yet) been achieved on the normative content of that concept. They argue that for this reason jus cogens must be treated as existing merely on paper. Hence, according to the sceptics, jus cogens is a term used only for rhetorical purposes. It lacks all reference in positive law*". LINDERFALK, U. *The Effect of* Jus Cogens *Norms: Whoever Opened Pandora's Box, Did You Ever Think About the Consequences?* The European Journal of International Law, vol. 18 no.5; pp. 853-871, en particular, p.855.

644 Informe de la Comisión de Derecho Internacional, adoptado en su 66º período de sesiones (5 de mayo a 6 de junio y del 7 de julio al 8 de agosto de 2014). Doc. A/69/10. P. 296.

645 Primer Informe de la Comisión de Derecho Internacional sobre el *jus cogens*, Preparado por Dire Tladi, Relator Especial, presentado en el 68º período de sesiones (del 2 de mayo al 10 de junio y del 4 de julio al 12 de agosto de 2016). Doc. A/CN.4/693. P.26.

de los Tratados. Así, su Relator Especial contabiliza hasta once referencias al mismo, de forma explícita, en fallos o providencias emitidos por la CIJ, así como en otros, de forma indirecta, como en el ya analizado, en capítulos precedentes del presente trabajo, caso sobre las Actividades Militares y Paramilitares en y contra Nicaragua; así como en dictámenes u opiniones consultivas emitidas por la CIJ, como hemos tenido en consideración, en relación el asunto de la Legalidad de la amenaza o el empleo de armas nucleares, entre otras. Tampoco han sido obviadas, más bien al contrario, en los votos particulares emitidos por los miembros de la CIJ, en el que se contabilizan setenta y ocho menciones expresas al *ius cogens*[646]. Quizás el argumento más incontestable que nos encontramos en el referido Primer Informe sea el que hace referencia a la aceptación por parte de los Estados implicados en una controversia internacional sobre la que la CIJ ejerce sus competencias, pues ningún Estado, en esas circunstancia, ha objetado el concepto del *ius cogens* , "incluso cuando habría redundado en su beneficio negar el *jus cogens* en ciertas causas, los Estados no lo hayan hecho"[647]. Como se evidencia en el referido Primer Informe, las polémicas en torno a la propia existencia del *ius cogens* quedan circunscritas al ámbito académico.

En cualquier caso, en el presente Capítulo partimos de la incontestable existencia de las normas de *ius cogens* como parte del Derecho Internacional vigente, por lo que deberemos atender a esas cuestiones sustantivas de las normas de *ius cogens* que aún son objeto de controversia para dilucidar si las normas de DIH que califican a determinados métodos de combate como prohibidos han alcanzado ese valor imperativo. A partir de entonces, podremos descubrir si sería de aplicación el artículo 26 de Proyecto de artículos sobre responsabilidad internacional. Es decir, si las normas de DIH que permiten calificar a un ciberataque como un método de combate prohibido hubiesen alcanzado ese carácter de *ius cogens,* no sería posible excluir la ilicitud del hecho, alegando cualquiera de las circunstancias o causas que excluyen la ilicitud del hecho contenidas en el Capítulo V del Proyecto de artículos.

---

[646] *Ibidem,*pp. 26-29.
[647] *Ididem,* p. 32.

2. CARACTERES DEL *IUS COGENS* Y SU CONSTATACIÓN EN LAS NORMAS PROHIBITIVAS DE DIH RELATIVAS A LOS MÉTODOS DE COMBATE.

La definición contenida en el artículo 53 de la Convención de Viena deja claramente los requisitos y caracteres del *ius cogens*, pues han de ser fruto de un consenso generalizado de la Comunidad internacional de Estados en su conjunto; no admiten acuerdo en contrario, caracterizando a estas normas como imperativas; y se sitúan en un plano superior al resto de las normas jurídicas internacionales, en cuanto que son inderogables en relación con la especial naturaleza del objeto, por lo que sólo van a ser modificadas por otra norma ulterior de derecho internacional general que tenga tal carácter.

Resulta necesario, pues, averiguar si esos caracteres pueden ser constatados en relación con las normas de DIH que permitirían calificar a un ciberataque como método de combate prohibido.

2. 1. La universalidad de las normas de *ius cogens*.

La universalidad o generalidad de las normas imperativas puede ser atendida desde una doble dimensión: la generalidad, en relación con el proceso de formación de las referidas normas, y la aplicación *erga omnes* de las mismas, con independencia de haber participado del consenso generalizado para su creación.

2.1.1. El consenso generalizado en su proceso de formación.

En relación con el proceso de formación de una norma imperativa o de *ius cogens*, hemos de recordar que el referido artículo 53 de la Convención de Viena establece que alcanzará tal carácter imperativo la norma que sea "*aceptada y reconocida por la comunidad internacional de Estados en su conjunto*". Como se indica en el Informe Anual de la CDI de 2014, la incorporación de estos términos ofrece

algo de claridad sobre algunos de los aspectos del proceso de formación de las normas de *ius cogens,* por lo que se puede dar a entender "que la aceptación por el conjunto de los Estados es un requisito del *"jus cogens"* [648] .La primera dimensión de la generalidad o universalidad evidencia la necesidad de gozar de un consenso generalizado que no implica la aceptación unánime de todos y cada uno de los Estados que forman parte de esa Comunidad Internacional.

Sin embargo, al considerar su proceso de formación, no han dejado de proliferar aportaciones doctrinales en las que se suscitan una serie de interrogantes adicionales como, por ejemplo: "*¿Cuántos Estados se requieren para considerar que hay una "comunidad de Estados en su conjunto"?* o *¿Se hace referencia a la totalidad de Estados o solamente a los Estados parte de la Organización de Naciones Unidas?*[649]".

En los esfuerzos realizados por la doctrina internacionalista para alcanzar una definición algo más precisa, la Comunidad Internacional ha sido entendida como "*aquel grupo de Estados miembros de las Naciones Unidas: la inmensa mayoría en el planeta*", habida cuenta que "*estos son los verdaderos participantes directos en la creación del orden público y la normatividad internacionales.*" [650]

En cualquier caso, la generalidad en el proceso de formación de la norma, como se ha indicado, no puede implicar una aspiración a la unanimidad, pues ningún sentido tendría reconocer la naturaleza imperativa únicamente a las normas que son adoptadas por la unanimidad de los Estados de la Comunidad Internacional. En caso de ser así, se perdería la ocasión de imponer su contenido a quienes rechazan el cumplimiento de las obligaciones más esenciales para la pervivencia de la propia humanidad. Sin embargo, aun tomando como punto de partida una tesis tan restrictiva como la que aquí se examina, puede desvelarse el

---

[648] Informe de la Comisión de Derecho Internacional, adoptado en su 66º período de sesiones…, Doc. cit; p. 298.

649 ABELLO-GALVIS, R., *Introducción al estudio de las normas de ius cogens en el seno de la Comisión de Derecho Internacional*, CDI. Universitas. Bogotá (Colombia) núm. 123, julio-diciembre de 2011; pp. 75-104, en particular, p.89.

650 ECHEVERRI P., *Ius cogens en sentido estricto y en sentido lato: Una propuesta para fortalecer la consecución de la paz mundial y la garantía del Corpus Iuris Internacional de protección al ser humano*. Memorando de Derecho. Año 2 núm. 2. 2011; pp. 205-223, en particular, pp. 211 y 212.

hecho de que sería, precisamente el DIH, el único cuerpo perteneciente al Derecho Internacional que podría cumplir tal requisito, pues "*las Convenciones de Ginebra de 1949* [son los] *únicos instrumentos multilaterales ratificados por los 194 Estados del mundo*[651]", a lo que podríamos añadir su innegable naturaleza consuetudinaria de ámbito general.

En el ámbito que nos ocupa GUTIÉRREZ ESPADA, circunscribe la imperatividad de la norma que prohíbe el uso de la fuerza a "*la aceptación de los tres principales grupos de Estados a estos efectos: el occidental, el "socialista" y el Tercer Mundo*[652]". De este modo, la vinculación de la generalidad de la norma en su formación y cumplimiento, aparece ya esencialmente unida a la superioridad de los fines que la misma protege y que se verá más adelante.

Por otra parte, la naturaleza consuetudinaria de gran parte de las normas que conforman el DIH obliga a realizar aquí una serie de consideraciones adicionales[653].Como ha podido verse, al examinar el contenido de la obligación internacional violada, las principales normas que regulan el uso de la fuerza durante un conflicto armado internacional o no internacional, han adquirido rango de Derecho consuetudinario y, en este sentido, LINDERFALK incluso afirma que "*stated somewhat differently, a norm of jus cogens may be said to presuppose the existence of two kinds of opinio juris*"[654].

---

651 *Ibidem*, p. 218.

652 GUTIÉRREZ ESPADA, C., La responsabilidad internacional del Estado por uso de la fuerza armada (la conformación del hecho ilícito internacional). Cursos de Derecho Internacional de Vitoria-Gasteiz, 1989. Servicio editorial de la Universidad del País Vasco, Bilbao, 1990; pp. 189-310, en particular, p. 223.

653 "*El ius cogens propiamente dicho tiene una naturaleza consuetudinaria, aunque no tiene por qué ser exclusiva*". CEBADA ROMERO, A., Los conceptos de obligación erga omnes, ius cogens y violación grave a la luz del nuevo proyecto de la CDI sobre responsabilidad de los Estados por hechos ilícitos. Revista Electrónica de Estudios Internacionales, núm. 4. Junio 2002; p. 6. Disponible en el sitio web: http://www.reei.org/index.php/revista/num4/agora/conceptos-obligacion-erga-omnes-ius-cogens-violacion-grave-luz-nuevo-proyecto-cdi-sobre-responsabilidad-estados-hechos-ilicitos. Fecha de consulta, marzo de 2013.

654 Defiende el autor que esta doble exigencia fue puesta de relieve en el análisis de la legalidad de las actividades británicas y americanas en Afganistán, pues entiende que, en el desarrollo de las mismas, el contenido del derecho a la legítima defensa, así como del propio concepto de ius cogens, sufrió cambios. "Obviously, it would not be enough if we could show that in this very period states changed their opinion with regard to the contents of the right of self-defence. We would also have to show that states changed their opinion with regard to the contents of peremptory international law. Considering the circumstances, this second requirement can hardly be met. (…) it is indeed an absurdity to imagine that in such a short

En consecuencia, atendido este requisito que se predica de las normas imperativas, puede concluirse que el mismo es, también, atribuible a las normas de DIH, por tratarse de un ámbito en el que consenso de la Comunidad Internacional en su conjunto es incuestionable[655].

Sin embargo, el artículo 53 de la Convención de Viena no especifica más sobre el proceso de formación de una norma de *ius cogens,* máxime cuando ésta pueda tener su origen en una previa norma consuetudinaria de ámbito universal, como lo son las normas del DIH que calificarían a un ciberataque como un método de combate prohibido. No obstante, en los debates que se produjeron en el seno de la CDI, al presentar el Sr. Tladi el Primer Informe sobre el *ius cogens*, tal y como se recoge en el Informe Anual de la CDI de 2016, se indicó que:

> "(…) las normas de *ius cogens* eran esencialmente normas de derecho internacional consuetudinario con una forma especial de *opinio iuris*, a saber, la convicción de la existencia de un derecho o una obligación jurídica de carácter imperativo. Por tanto, esas normas constituyen una práctica general aceptada como derecho imperativo. En otras palabras, una práctica general acompañada de *opinio iuris cogens"*[656].

Esta importante cuestión será objeto de atención por el Relator Especial en sus próximos Informes sobre el *ius cogens*, así como la atención a los tratados internacionales como posibles generadores de normas imperativas o su interacción al ser reflejadas tales normas en los tratados; y también el hecho de que las normas de *ius cogens* puedan basarse en los principios generales del derecho.

---

period of time a similar development could ever be effected with regard to a norm of jus cogens. It is entirely inimical to the idea of jus cogens as an uncommonly permanent set of norms". LINDERFALK, U. *The Effect of* Jus Cogens *Norms: Whoever Opened Pandora's Box, Did You Ever Think About the Consequences?,* op. cit.; pp. 862 y 863.

655 Sin olvidar que, como manifiesta NIETO-NAVIA, "*What is most important is that "only some subjects of international law, acting alone or in conjunction with others" cannot create jus cogens and thereafter impose their interpretation on the majority of States*". NIETO-NAVIA, R. International Peremptory Norms (Jus Cogens) and International Humanitarian Law. CASSESE, A., VOHRAH, L. C., Man's inhumanity to man: essays on international law in honour of Antonio Cassese. London 2003; pp. 595-640, en particular, p. 606.

656 Informe de la Comisión de Derecho Internacional, adoptado en su 68º período de sesiones (del 2 de mayo al 10 de junio y del 4 de julio al 12 de agosto de 2016). Doc. A/A/71/10. P. 324.

2.1.2. La aplicación universal de las normas imperativas.

La segunda dimensión de la generalidad va dirigida a su ámbito de aplicación universal. Es decir, que al margen de que se haya participado de ese consenso generalizado, las normas imperativas son de obligado cumplimiento para todos y cada uno de los Estados que conforman la Comunidad Internacional. En este sentido, la universalidad de su cumplimiento está directamente vinculada a la distinción entre obligaciones contraídas entre Estados y las obligaciones *erga omnes.* Sin embargo, no ha de procederse a una asimilación simplista entre las normas imperativas y las normas *erga omnes,* pues, aunque es evidente que las primeras surten efectos *erga omnes,* no todas las normas *erga omnes* han adquirido un carácter imperativo. Como indica AGUILAR CAVALLO,

> "[…] cuando hablamos de las obligaciones *erga omnes*, estamos en el campo de la aplicación y/o cumplimiento del Derecho Internacional, de la obligación de respetar y hacer respetar el Derecho Internacional y de los titulares de la acción de respeto del Derecho Internacional, mientras que las normas de *ius cogens* no juegan su rol principal en el área de la aplicación del Derecho Internacional. Las normas de *ius cogens* son consideradas tales por el hecho de que por sus propias características son jerárquicamente superiores al resto de las normas"[657].

Uno de los aspectos que tendrá que atender el Relator Especial en sus futuros Informes sobre el *ius cogens*, a instacia de la CDI, será la relación entre las normas imperativas y las obligaciones *erga omnes*[658].

En cualquier caso, si atendemos a lo que hemos venido a denominar doble dimensión de la universalidad del *ius cogens* internacional, el hecho de que nos encontremos ante normas fruto de un consenso generalizado y que surtan efectos *erga omnes* no resulta un elemento identificador de las normas de *ius cogens* salvo que sea atendida esa universalidad en conjunción con la imperatividad. En

[657] AGUILAR CAVALLO, G., El reconocimiento jurisprudencial de la tortura y de la desaparición forzada de personas como normas imperativas de derecho internacional público, en *Revista Ius et Praxis,* vol.12, nº 1, Talca, 2006; p. 123. (pp.117-154 para bibliografía).
[658] Informe de la Comisión de Derecho Internacional, adoptado en su 68º período de sesiones …, doc.cit; p.327.

consecuencia, aunque las normas convencionales y consuetudinarias de DIH aplicables para la calificación de un ciberataque como método de combate prohibido cumplan con el requisito de la generalidad, en ambas dimensiones, deberemos descubrir si, además, concurre una *opinio iuris cogens*, en el sentido antes recogido en el Informe Anual de la CDI de 2016.

2.2. La imperatividad de las normas de *ius cogens*.

A la vista del artículo 53 de la Convención de Viena, las normas imperativas "no admiten acuerdo en contrario". Es decir, impiden la actuación del libre consentimiento de los Estados, que no puede imponerse a su contenido. Se trata, por lo tanto, de una excepción a la actuación estatal y que implica la imposibilidad de que dicho consentimiento pueda surtir ningún efecto jurídico. En este sentido, nos encontramos ante una excepción al conjunto de normas de Derecho Internacional que son creadas, modificadas y abrogadas por actos consensuales. En efecto, como se indica en el Primer Informe sobre el *Ius cogens,* la mayoría de las normas internacionales son *ius dispositivum*, "en tanto, excepcionalmente, algunas tienen el carácter de *jus cogens* "[659]

El hecho de que las normas de *ius cogens* no admiten acuerdo en contrario refleja claramente que nos encontramos ante el excepcional elemento quebrantador el principio del libre consentimiento sobre el que se fundamentan la mayoría de las normas internacionales de *ius dispositivum.* Este carácter imperativo está estrechamente vinculado con el último de los caracteres que atenderemos en el siguiente epígrafe: la superioridad, consecuencia de la inderogabilidad de las mismas y la naturaleza misma de su objeto. En este sentido podemos afirmar que la validez del resto del conjunto normativo internacional dependa de su concordancia con las normas de *ius cogens.*

En consecuencia, la existencia de normas imperativas afectará no sólo al ámbito convencional, sino también al consuetudinario y a los propios principios generales del Derecho. Es más, incluso en relación con los actos unilaterales de los Estados, pues no podrán surtir efectos jurídicos si van en contra de una

[659] Primer Informe de la Comisión de Derecho Internacional sobre el *Ius cogens,…,* doc.cit. p.43.

norma de *ius cogens.*

La vinculación del *ius cogens* con las normas convencionales internacionales es innegable, como lo demuestra su inclusión en la Convención de Viena de 1969. De este modo, la inadmisión de acuerdo en contrario extiende sus efectos respecto de cualquier obligación convencional, libremente asumida por los Estados, con severas consecuencias jurídicas, como es la nulidad absoluta del tratado (art.53 de la Convención de Viena), cuando se intente imponer el consentimiento estatal contraviniendo una norma de *ius cogens* existente en el momento de celebración del referido tratado. Importantes consecuencias jurídicas se pueden producir, incluso, cuando el consentimiento de los Estados fue conforme al *ius cogens* vigente en el momento de celebración del tratado, pues "*si surge una nueva norma imperativa de derecho internacional general, todo tratado existente que esté en oposición con esa norma se convertirá en nulo y terminará*" (art. 64 de la Convención de Viena)

En el mismo sentido, se establece en el artículo 26 del Proyecto de artículos sobre responsabilidad internacional, la imposibilidad de justificar la ilicitud de un hecho, si se produce en violación de una norma de *ius cogens*. El capítulo V del Proyecto comienza admitiendo el libre consentimiento del Estado lesionado, como causa justificativa del hecho ilícito del Estado agresor, salvo que el mismo se otorgue en relación a la violación de una norma imperativa.

Como ocurría en el análisis del anterior rasgo característico, la inadmisibilidad de un acuerdo en contrario resulta estrechamente relacionada con la superioridad de los intereses protegidos por la norma imperativa pues, de otro modo, el libre consentimiento de los Estados, no vería justificada su ineficacia.

Así, como afirma ACOSTA ESTEVEZ, las normas de *ius cogens*, en contraposición a las normas dispositivas, no admiten acuerdo en contrario por cuanto, "*protegen los intereses fundamentales o esenciales que la comunidad internacional precisa para su supervivencia y, en consecuencia, imposibilitan a los sujetos*

el sustraerse de las mismas[660]." Y, por último, no puede olvidarse que habrá situaciones en que, como afirma CEBADA ROMERO, "*la gravedad derivará exclusivamente de la importancia suprema del valor protegido*[661]".

Es decir, la imperatividad de las normas no encuentra su fundamento en un argumento formal, sino en su propia razón de existir, identificada con la pervivencia de la misma humanidad. De este modo, puede afirmarse que, al mismo tiempo que una limitación a la libre voluntad estatal, las normas imperativas constituyen el máximo reconocimiento del mismo, pues nos encontramos ante materias en las que los Estados, a través de esa generación universal de la norma, han asumido libremente la existencia de una serie de intereses superiores, cuya protección ha de garantizarse por encima de la libre voluntad de los mismos.

2.3. La superioridad de las normas de *ius cogens*.

Hasta ahora, el examen de los presupuestos previos ha mostrado la necesidad de un consenso generalizado y de la imposibilidad de que dicho consenso resulte mutado por la libre voluntad de los Estados, para que pueda hablarse de normas imperativas. No obstante, ninguno de estos caracteres hallaría su completa razón de ser en ausencia de la superioridad que se predica en el tercero de los rasgos, presentes en la definición del artículo 53 de la Convención de Viena. El voluntarismo del Derecho Internacional encuentra, así, la mayor expresión en la inmovilidad de las normas imperativas, pues las mismas constituyen el núcleo del Derecho Internacional en el que el consenso alcanza la suficiente entidad, como para que la modificación de dichas normas resulte incuestionable.

Se trata, por lo tanto, de la materialización de una serie de valores respecto

660 ACOSTA ESTEVEZ, J.B., *Normas de ius cogens, efecto erga omnes, crimen internacional y la teoría de los círculos concéntricos.* Anuario de derecho internacional. XI, 1995; pp. 3-22, en particular, p.5.
661 Tal es el caso, a juicio de la autora, cuando "*se incumple la obligación de abstenerse del uso de la fuerza. En este caso basta con una única vulneración del principio para que el ilícito sea calificado como grave. Otras veces, en cambio, junto a la esencialidad del valor protegido se exige una particular intensidad de la violación para que esta pueda definirse como grave. Esto es lo que ocurre en relación con la obligación de respetar los derechos humanos fundamentales*". CEBADA ROMERO, A. *Los conceptos de obligación erga omnes, ius cogens y violación grave a la luz del nuevo proyecto de la CDI sobre responsabilidad de los Estados por hechos ilícitos*, op. cit; p. 9.

de los que el consenso alcanzado por los Estados favorece el reconocimiento de un núcleo del Derecho Internacional indisponible[662]. En el caso concerniente a la aplicación de la Convención sobre la prevención y castigo del crimen de Genocidio, la CIJ reitera tales argumentos, afirmando que[663]:

> *«(...). The first consequence arising from this conception is that the principles underlying the Convention are principles which are recognized by civilized nations as binding on States, even without any conventional obligation. A second consequence is the universal character both of the condemnation of genocide and of the cooperation required 'in order to liberate mankind from such an odious scourge' (Preamble to the Convention)»*[664]

En la cuestión que aquí atañe, es preciso desentrañar si esos valores o principios superiores se encuentran entre los que conforman el DIH para determinar si las normas que componen el DIH, convencional y consuetudinario, comparten esta naturaleza imperativa. En consecuencia, es necesario analizar, en primer lugar, si el uso de la fuerza reúne los caracteres que aquí se muestran y, en su caso, en qué medida. En un principio puede afirmarse que la observancia de la norma que prohíbe el uso de la fuerza resulta determinante para la pacífica convivencia de la Comunidad Internacional. Los trabajos de la CDI, en relación al Proyecto de artículos sobre responsabilidad de los Estados, manifiestan asimismo, la naturaleza imperativa de esta norma, al afirmar: "*en la época actual todo uso por un Estado de la fuerza armada que se traduzca en uno de los atentados indicados contra la soberanía de otro Estado cae bajo el concepto de «agresión» y, como tal, es objeto de una prohibición de jus cogens, de la más típica e indiscutible prohibición de jus cogens, tanto en el derecho internacional general como dentro del sistema de las*

662 Para NIETO-NAVIA, "*These laws develop or are created not by an international legislator or sovereign, but very generally through the consensus of States which have recognized that certain 'values' amount to valid legal norms which must be respected as between States.14 In this regard, it is possible to talk of the 'validity' of international law*". NIETO-NAVIA, R., *International peremptory norms (jus cogens) and International Humanitarian Law*, op. cit; p. 2.

663 CHETAIL, V., *The contribution of the International Court of Justice to international humanitarian law*. International Review of the Red Cross. June 2003 , vol. 85 no 850; pp.235-269, en particular, p..249.

664 Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Case concerning application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia) (Preliminary objections), ICJ Reports 1996, para. 31.

Naciones Unidas[665]."

Sin embargo, a la vista de las normas aplicables al conflicto y que constituyen el DIH no puede concluirse que todo uso de la fuerza se encuentre prohibido y que esta obligación no sea del todo disponible por los Estados[666].

Es aquí donde cobra de nuevo relevancia la determinación de los intereses que se hallan especialmente protegidos por el *ius cogens*, pues, éstos han de "*representar a uno de los grupos de intereses relevantes para la configuración del interés fundamental del que deriva la obligación violada*"[667] .

El fundamento de la imperatividad de las normas de DIH ha sido reconocido en el contenido y aplicación de la Cláusula Martens[668], al entenderse que las normas de DIH, incluidas en los Anexos al IV Convenio de la Haya de 1907, fueron "*recognized by all civilized nations and were regarded as being declaratory of the laws and customs of war*"[669].

Por otra parte, la imposibilidad de disposición por los Estados, del contenido de estas normas, impide su derogación a través del ejercicio del libre consentimiento de los Estado. Sin embargo, ello no puede abocar a afirmar una absoluta inderogabilidad de estas normas. Antes bien, como consecuencia de su superioridad, ha de admitirse que, en efecto, se trata de normas derogables, con la limitación impuesta en el propio artículo 53, que la circunscribe a aquéllas

---

665 Adición al octavo informe sobre la responsabilidad de los Estados. Relator, AGO, R. Documento A/CN.4/318/add.5 a 7; par. 55.

666 Para GUTIERREZ ESPADA, no puede afirmarse el carácter imperativo global o total de la norma que prohíbe el uso de la fuerza, sino sólo de aquéllas que constituyen las violaciones más graves. GUTIÉRREZ ESPADA, C., *La responsabilidad internacional del Estado por uso de la fuerza armada (la conformación del hecho ilícito internacional)*, op. cit.; p. 223.

667 CARDONA LLORENS, J. *La responsabilidad internacional por violación grave de obligaciones esenciales para la salvaguarda de intereses fundamentales de la comunidad internacional. (EL «CRIMEN INTERNACIONAL»)*; op. cit.; p. 283.

668 CHETAIL, así lo argumenta al afirmar que: "*The (Martens) Clause may indeed be understood in two different ways. First, it may merely be intended to recall the continued relevance of customary law when treaty law is not applicable, in which case the "principles of humanity" and the "dictates of public conscience" referred to in the Clause would be redundant and would only provide the ethical foundations of the customary laws of war. Secondly, it may however be argued that the "principles of international law" referred to in the Clause are derived from three different and autonomous sources, namely "established custom", the "principles of humanity" and the "dictates of public conscience". Arguably, the Martens Clause enables one to look beyond treaty law and customary law, and to consider principles of humanity and the dictates of the public conscience as separate and legally binding yardsticks*". CHETAIL, V., *The contribution of the International Court of Justice to international humanitarian law*, op. cit.; p.258.

669 NIETO-NAVIA, R., *International peremptory norms (jus cogens) and International Humanitarian Law*, op. cit.; pp. 21 y 22.

normas "*que tengan el mismo carácter, reconocidas como tales por la comunidad internacional en su conjunto, y de ahí que no se admita en el caso del Derecho internacional imperativo el argumento de la objeción persistente para sustraerse a la aplicación de la norma*"[670]. En consecuencia, para poder modificar una norma de *ius cogens* se requiere una norma que tenga el mismo valor y, por lo tanto, "*solo puede ser modificada por una norma que tenga la misma jerarquía y, obviamente, que la Comunidad Internacional de Estados la haya aceptado como tal*"[671].

En este sentido, en el Primer Informe sobre el *ius cogens* se establece claramente cómo ha de interpretarse la "inderogabilidad" de las normas de *ius cogens,* al manifestar, en su parágrafo 62 que:

"El elemento de inderogabilidad cumple una doble función. En primer lugar, es una consecuencia de la imperatividad. Sin embargo, también es un elemento importante de la naturaleza del *jus cogens*. […] la inderogabilidad es el núcleo de la idea del *jus cogens*"[672].

Como se afirma en ese Primer Informe, la inderogabilidad está estrechamente vinculada a la superioridad jerárquica, pues "(…) las normas de *ius cogens* son jerárquicamente superiores a otras normas del derecho internacional"[673]. No obstante, como se manifestó en los debates que se produjeron en el seno de la CDI sobre ese Primer Informe, "el rasgo distintivo (…) de las normas de *ius cogens* no era tanto su naturaleza jerárquica, sino más bien su especial importancia"[674]

Sin embargo, el hecho de que las normas de DIH y las de *ius cogens* compartan ciertas notas, no puede hacer concluir de forma apriorística que todas las normas de DIH sean imperativas[675]. Por el contrario, dentro del acervo

670 CEBADA ROMERO, A. *Los conceptos de obligación erga omnes, ius cogens y violación grave a la luz del nuevo proyecto de la CDI sobre responsabilidad de los Estados por hechos ilícitos*, op. cit.; p. 4.
671 ABELLO-GALVIS, R. *Introducción al estudio de las normas de ius cogens en el seno de la Comisión de Derecho Internacional*, op. cit.; p.91.
672 Primer Informe de la Comisión de Derecho Internacional sobre *ius cogens,* doc.cit; p.42.
673 *Ibidem*; p.47.
674 Informe de la Comisión de Derecho Internacional, adoptado en su 68º período de sesiones, doc.cit; p.326.
675 Asi se expresa también VERDROSS, quien entiende que un grupo importante de normas de derecho internacional general creadas con propósitos humanitarios tienen el carácter de ius cogens y otro grupo de normas que tienen este carácter son los introducidos en la Carta (art. 2 y 51). VERDROSS, A., *Jus dispositivum and jus cogens in international law*, op. cit; pp. 59-60.

constituido por el DIH, habrá que delimitar qué normas forman parte del *ius cogens*.

En este propósito, hay que acudir al Proyecto de artículos sobre responsabilidad internacional de los Estados, en cuyo Capítulo III, titulado "*Violaciones graves de obligaciones emanadas de normas imperativas del derecho internacional general*", se afirma que "*El presente capítulo se aplicará a la responsabilidad internacional generada por una violación grave por el Estado de una obligación que emane de una norma imperativa del derecho internacional general*". En el artículo 40.2, por su parte, aclara qué ha de entenderse por violación grave, al establecer que "*La violación de tal obligación es grave si implica el incumplimiento flagrante o sistemático de la obligación por el Estado responsable*". En relación a este artículo, la CDI, en sus Comentarios al Proyecto de artículos, entiende inapropiado ofrecer ejemplos que delimiten las normas imperativas. Sin embargo, aclara que estas obligaciones "*dimanan de normas sustantivas de comportamiento que prohíben lo que ha llegado a considerarse intolerable porque representa una amenaza para la supervivencia de los Estados y para los valores humanos más fundamentales*"[676]. Asimismo, aun sin carácter exhaustivo, la CDI enumera determinadas normas que, indudablemente, revisten carácter imperativo, mencionando, entre ellas, la prohibición de la agresión, la prohibición de la esclavitud y el genocidio[677].

Especial mención merece, en este punto, la posibilidad apuntada por la propia CDI, en relación a las normas de DIH, pues, aunque no afirma, como en los casos precedentes, su carácter imperativo de forma categórica, deja una puerta abierta a dicho reconocimiento. Así, señala que, toda vez que la CIJ ha declarado como ""*inconculcables*", *las normas básicas de DIH aplicables en los conflictos armados*", de modo que "*parecería estar justificado que se considerasen también imperativas*[678]".

En este punto, puede resultar ilustrativa la Jurisprudencia internacional, aunque en relación al carácter imperativo de las normas de DIH, las decisiones

676 Comenatrio 3) al artículo 40 del Proyecto.
677 Comentarios 4) y 5) al artículo 40 del Proyecto.
678Comentario 5) al artículo 40 del Proyecto.

de la CIJ no han sido todo lo esclarecedoras que hubiera sido deseable. Sin embargo, dichas decisiones sí pueden tomarse como referencia y base primigenia en la defensa de la existencia de un número escaso de normas de DIH que, por estar destinadas a proteger los valores más esenciales de la humanidad, han de reputarse de *ius cogens*.

Así, en la Opinión Consultiva emitida por la CIJ en relación con las Reservas a la Convención sobre la Prevención y Castigo del Crimen de Genocidio, el citado órgano entiende que:

> «The Convention was manifestly adopted for a purely humanitarian and civilizing purpose. It is indeed difficult to imagine a convention that might have this dual character to a greater degree, since its object on the one hand is to safeguard the very existence of certain human groups and on the other to confirm and endorse the most elementary principles of morality. In such a convention the contracting States do not have any interest of their own; they merely have, one and all, a common interest, namely, the accomplishment of those high purposes which are the raison d'être of the convention. Consequently, in a convention of this type one cannot speak of individual advantages or disadvantages to States, or of the maintenance of a perfect contractual balance between rights and duties. The high ideals which inspired the Convention provide, by virtue of the common will of the parties, the foundation and measure of all its provisions»[679].

Esos altos ideales que se citan en la referida Sentencia, podrían verse reconocidos en las normas de DIH. En este sentido, puede resultar ilustrativa la repetida Opinión Consultiva dictada en relación a la licitud de las armas nucleares, en la que la CIJ puso especial énfasis en la importancia de las normas de DIH, así como en la particularidad de dichas normas, en relación con el resto de las que componen el Derecho Internacional Consuetudinario ordinario[680]. Si bien es cierto que, como expone CHETAIL, la expresión "*principios intransgredibles*" podría resultar enigmática, al poder ser objeto de

679 Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide, doc. Cit; p. 23.
680 CHETAIL, V. *The contribution of the International Court of Justice to international humanitarian law*, op. cit; p.251.

interpretación[681]. Así, si por un lado queda claro que la Corte sostuvo el carácter consuetudinario del DIH, sin embargo, ese carácter intransgredible de determinadas normas, no siempre ha sido asimilado a su naturaleza imperativa [682]".

Si se retoma la controvertida Opinión Consultiva relativa a la licitud del empleo de las armas nucleares, asimismo, se comprueba que la CIJ, al analizar el uso de la fuerza, ejercido en legítima defensa estableció que "*according to the law of self-defence, in order for a use of force to be proportionate, it must meet 'the requirements of the law applicable in armed conflict which comprise in particular the principles and rules of humanitarian law*' [683]." A juicio de LINDERFALK, para la CIJ se trataba únicamente de dejar claro que "*substantial parts of international humanitarian law, too, would have to be characterized as jus cogens*".[684]

Si bien es cierto que de las decisiones emanadas por la CIJ no puede desprenderse un catálogo de normas de DIH, que puedan ser calificadas como *ius cogens*, no lo es menos que la Corte se ha referido a éstas con diversas expresiones que permiten, al menos, apuntar cuáles puedan ser. Así la CIJ al tratar estas normas de DIH ha invocado conceptos tales como «*elementales consideraciones de humanidad*», «*principios que obligan a los Estados al margen de todo vínculo convencional*», «*los intereses de la humanidad en general*», la idea de «*misión*

---

681 CHETAIL entiende que dicha expresión puede ser interpretada de dos modos, "*On the one hand, the Court could be suggesting that fundamental principles of humanitarian law constitute norms of jus cogens in statu nascendi, which are on the point of becoming peremptory norms of international law but cannot yet be plainly considered as such. It can be argued, on the other hand, that by underlining the intransgressible character of the fundamental rules of humanitarian law, the Court implicitly admits the peremptory character of such rules, but refrains from doing so explicitly, because it is dealing with the more limited issue of the applicability of such norms to the case under consideration. Following the same line of reasoning, some judges go one step further and acknowledge in clear terms that the principles and rules of international humanitarian law do have the character of jus cogens. President Bedjaoui holds, in his Separate Opinion, that the majority of rules of humanitarian law have to be considered as peremptory norms of international law. Judge Weeramantry, in his Dissenting Opinion, states categorically that: "The rules of the humanitarian law of war have clearly acquired the status of ius cogens, for they are fundamental rules of a humanitarian character, from which no derogation is possible without negating the basic considerations of humanity which they are intended to protect*"". *Ibidem*; p.251.

682 A pesar de ello, como sostiene ABELLO- GALVIS "a*l respecto, Luigi Condorelli nos dice que intransgredible (sic) no significa imperativo, aunque sostiene que la CIJ sí aproximó los conceptos de DIH y ius cogens*", ABELLO-GALVIS, R. *Introducción al estudio de las normas de ius cogens en el seno de la Comisión de Derecho Internacional*, op. cit; p. 97.

683 LINDERFALK,U. *The Effect of* Jus Cogens *Norms: Whoever Opened Pandora's Box, Did You Ever Think About the Consequences?,* op. cit; p. 865.

684 *Ibidem*, p. 866.

sagrada de civilización», y «*carácter fundamental*»[685]. Por lo tanto, conjugando dichas expresiones con las elementales normas que han sido estudiadas en la Primera Parte del presente trabajo, no parece desacertado concluir que dichos caracteres, pudieran asimilarse, en un principio, con los que se han expuesto en relación con las normas imperativas.

Sin embargo, no resultó tan contundente la CIJ en su pronunciamiento relativo a la tan citada Opinión Consultiva, emitida con ocasión de la consulta realizada en torno a la licitud del empleo de las armas nucleares pues, en dicha Opinión , afirmó que "*there was no need for it to deal with the issue of whether such rules are part of jus cogens or not*". A juicio de CHETAIL, en este caso, la Corte desaprovechó la oportunidad de clarificar la naturaleza de ius cogens del DIH[686]". Sin embargo, ya ha quedado apuntado, como la Comisión ha entendido que la afirmación, por parte de la CIJ de que: "*[The] fundamental rules [of humanitarian law] are to be observed by all States whether or not they have ratified the conventions that contain them, because they constitute intransgressible principles of international customary law*[687]", puede entenderse como una puerta abierta al posible reconocimiento de la imperatividad de determinadas normas de DIH.

Comparten con el resto de obligaciones imperativas de Derecho Internacional la nota característica de que su protección afecta a los intereses de la Comunidad Internacional en su conjunto[688], como por otra parte, ya se recogía en los llamados "Principios de Nuremberg" donde puede encontrarse una enumeración cuya esencia comparten los textos citados[689].

---

685 Así lo recoge QUISPE en, QUISPE REMÓN, F. *Las normas de ius cogens: ausencia de catálogo.* Anuario español de Derecho Internacional, vol. 28, 2012; pp. 143-183, en particular, p.162.

686 Véase, CHETAIL, V., *The contribution of the International Court of Justice to international humanitarian law*, op. cit.; p.250.

687 Legality of the Threat or Use of Nuclear Weapons, doc. cit.; par. 79.

688 Para BASSIOUNI, "*certain crimes affect the interests of the world community as a whole because they threaten the peace and security of humankind and because they shock the conscience of humanity*". BASSIOUNI, C., *International Crimes: Jus Cogens and Obligatio Erga Omnes.* Law and Contemporary Problems, vol. 59. Fall 1996; pp. 63-74, en particular, p. 69.

689 NUÑEZ PALACIOS subraya que, en dichos Principios se establece que los crímenes de guerra son: "principalmente violaciones a las leyes o costumbres de guerra que incluyen, entre otras, asesinatos, malos tratos o deportación para trabajos forzados o para cualquier otro propósito de la población civil de o en territorio ocupado; asesinato o malos tratos de prisioneros de guerra o personas en alta mar, muerte de rehenes, saqueo de la propiedad pública o privada, destrucción de ciudades, poblaciones y pueblos o devastación no justificada por necesidades

Además, la caracterización como norma de *ius cogens*, sitúa a la misma en la cúspide de la pirámide normativa internacional[690] y, ello, es plenamente aceptable respecto de las normas enunciadas por el CICR, que se estudiarán en un apartado posterior[691].

No obstante, como se anticipaba, no parece que la totalidad de las normas de DIH hayan de ser incluidas entre las normas de *ius cogens*, antes bien, determinadas obligaciones, presentes en los Convenios de Ginebra y sus Protocolos Adicionales y en la Compilación de DIH Consuetudinario, podrán tener, indudablemente, carácter *erga omnes,* pero esto no será suficiente para predicar de todas ellas la condición de normas imperativas[692]. Antes al contrario, recogiendo el argumento de CEBADA ROMERO, "*el Derecho imperativo, configurado con estas características, siempre origina obligaciones erga omnes que reunen los dos elementos constitutivos a los que se refería el TIJ en el asunto Barcelona Traction*[693]". Es decir, la norma imperativa siempre producirá efectos *erga omnes* sin que pueda firmarse el argumento contrario de hacer pretender que toda norma *erga omnes* sea imperativa.

---

militares". NÚÑEZ PALACIOS, S. *El incumplimiento del Derecho Humanitario - Acciones internacionales*. 24 de febrero de 1999. Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/5tdmr6.htm
Fecha de consulta, marzo de 2013.

690 WOUTERS, J. y VERHOEVEN, S. al respecto manifiestan que: "*As they aim at protecting the fundamental interests of the international community, norms of ius cogens come at the top of the hierarchy of norms in international law*". WOUTERS, J. and VERHOEVEN, S., The Prohibition of Genocide as a Norm of Ius Cogens and Its Implications for the Enforcement of the Law of Genocide. International Criminal Law Review, vol. 3, 2005; pp. 401–416, en particular, 411.

691CICR, Grave breaches specified in the 1949 Geneva Conventions and in additional Protocol I of 1977. Documento de fecha 31 de enero de 1998. Disponible en el sitio web: https://www.icrc.org/eng/resources/documents/misc/57jp2a.htm. Fecha de consulta, marzo 2013.

692 Tal y como entiende NIETO-NAVIA, "*Although it has been suggested that there is a strong presumption that at least the 'grave breaches' provisions of the four Geneva Conventions have gained peremptory status it has also been acknowledged that many of the norms contained within the conventions do not fulfil the criteria which are necessary for such a norm to be considered as jus cogens. The principles and prohibitions underlying paragraphs (1) and (2) of common Article 3 are truly peremptory in nature. (…)it lays down the "elementary considerations of humanity" described by the ICJ which derive "from established custom, from the principles of humanity and from the dictates of public conscience". (…)*" . NIETO-NAVIA, R. *International peremptory norms (jus cogens) and International Humanitarian Law*, op. cit.; pp. 25 y 26.

693 CEBADA ROMERO, A. *Los conceptos de obligación erga omnes ius cogens y violación grave a la luz del nuevo proyecto de la CDI sobre responsabilidad de los Estados por hechos ilícitos*., op. cit,; p. 4.

El Relator Especial sobre el *ius cogens* también hizo referencia, en su Primer Informe, a la cuestión de los valores amparados por estas normas, que considera los valores fundamentales de la comunidad de derecho internacional", vinculándolos a las consideraciones básicas de humanidad. Además, en el segundo apartado de la conclusión 3, en incluida en su Primer Informe, el Sr. Tladi estableció que "Las normas de *ius cogens* amparan los valores fundamentales de la comunidad internacional, son jerárquicamente superiores a otras normas de derecho internacional y son de aplicación universal"[694]. Sin embargo, en los debates que se produjeron en el seno de la CDI, tras la presentación del referido Informe, algunos miembros manifestaron sus discrepancias al respecto. Así, para algunos, la existencia del *ius cogens* la aceptación y el reconocimiento del mismo no dependía de una evaluación subjetiva de los valores. Mientras, para otros, esa referencia a los valores fundamentales "era demasiado restringida si solo se refería a las normas de *ius cogens* de carácter humanitario y excluía otras, como la prohibición del uso de la fuerza (…) se propuso que, en vez de ello, el proyecto de conclusión se refiriese a los principios fundamentales por excelencia"[695]. En cualquier caso, lo importante es que cuestiones tan relevantes como "la relación entre la existencia de valores fundamentales subyacentes al *ius cogens* y la expresión de su existencia"[696] sean atendidos en los próximos Informes, de acuerdo con el plan de trabajo presentado por el Relator Especial.

3. CRITERIOS DE IDENTIFICACIÓN DE LAS NORMAS DE *IUS COGENS*.

Como se ha expuesto, el criterio que identifica una norma imperativa no se basa en su inclusión en un listado, sino en la especial naturaleza del objeto que la norma protege. En consecuencia y, visto que no puede predicarse el carácter imperativo de la totalidad de las normas de DIH, habrá que ver si, una vez acreditados los requisitos anteriores, las mismas pueden hallar su

[694] Primer Informe de la Comisión de Derecho Internacional sobre *ius cogens*, doc.cit., p.50.
[695] Informe de la Comisión de Derecho Internacional, adoptado en su 68º período de sesiones, doc.cit; p.326.
[696] *Ibidem, p. 327.*

encuadramiento en el *ius cogens*. Es decir, como ha quedado apuntado, únicamente las normas de DIH que supongan una violación grave o una agresión, podrán ser consideradas imperativas, quedando para el resto, la condición de normas convencionales y consuetudinarias con efectos *erga omnes*.

En esta labor, destinada a la determinación de esa gravedad, resulta imprescindible acudir, de nuevo, al Proyecto de artículos sobre responsabilidad Internacional. Como hemos podido observar, hasta ahora, es innegable la estrecha vinculación entre el tema de la responsabilidad internacional de los Estados por comisión de hechos ilícitos y el *ius cogens*. Sin embargo, las aportaciones expresas por parte de la CDI están por llegar, pues el Relató Especial "confirmó que no tenía intención de pasar por alto las implicaciones del *ius cogens* en el contexto de la responsabilidad del Estado por hechos internacionalmente ilícitos (…) su idea inicial era ocuparse de esas cuestiones en informes posteriores sobre las consecuencias del *ius cogens"*[697]. En consecuencia, atenderemos a las aportaciones en materia de responsabilidad internacional.

A juicio de CARDONA LLORENS, la evolución de la Comunidad Internacional y del derecho que la regula, se manifiesta en la "*propuesta de responsabilidad por "crímenes internacionales", realizada en el art. 19 del Proyecto de artículos de la CDI"*[698]. En efecto, la distinción que el originario Proyecto realizaba entre crímenes y delitos internacionales, resulta determinante a la hora de reconocer los ámbitos de especial importancia de una sociedad internacional históricamente determinada.

El referido primer Proyecto artículos, en su artículo 19 definía el crimen internacional, enumerando cuatro conductas que serán objeto de análisis en orden a concluir si las mismas pueden o no ser cometidas a través de la violación de una norma de DIH, conforme a lo expuesto en el Capítulo Segundo del presente trabajo.

Así, el aludido artículo, en primer lugar, entiende que un crimen

---

[697] Informe de la Comisión de Derecho Internacional, adoptado en su 68º período de sesiones, doc.cit; p.328.

698 CARDONA LLORENS, J. La responsabilidad internacional por violación grave de obligaciones esenciales para la salvaguarda de intereses fundamentales de la comunidad internacional (el «crimen internacional»), op. cit.; p. 267.

internacional puede resultar, en particular: *a) de una violación grave de una obligación internacional de importancia esencial para el mantenimiento de la paz y la seguridad internacionales, como la que prohíbe la agresión*. Se trata aquí, pues, de la transgresión de la obligación internacional que prohíbe el uso de la fuerza, en la medida apuntada por el propio artículo. Es decir, que constituya un uso de la fuerza, equiparable a la agresión.

En relación a las normas de DIH, aplicables al cibercombate, ya veíamos cómo, a través de una ciberoperación, puede cometerse un ataque armado que conlleve la causación de resultados asimilables a los que pueden resultar de un ataque cometido por métodos de combate convencionales. Como quedó expuesto en el Capítulo Primero, un ciberataque puede constituir un crimen de agresión, a la luz de la revisión de dicho concepto, formulada en la conferencia de Kampala y que, inicialmente, se contenía en la Resolución 3314 de Naciones Unidas. En consecuencia, una ciberoperación, desarrollada en un conflicto armado y lanzada sin que pueda acreditarse ninguna necesidad militar, podrá constituir, *a priori*, una agresión y entrar, por ende, en la definición de crimen internacional que ofrecía el citado artículo.

En relación a la obligación de respetar la distinción entre civiles y combatientes, sin embargo, será preciso que dicha agresión sea un resultado de la falta de distinción. Podría darse, asimismo, el supuesto de que a través de un ciberataque, aun en conflicto armado, resultaran bajas en el ámbito civil, en violación de una obligación internacional de DIH, como reiteradamente se ha expuesto. Sin embargo, no puede afirmarse de plano que dicha violación lo sea de una norma imperativa, pues a la luz del criterio ofrecido por la definición de crimen internacional, la entidad de la violación carecería la gravedad requerida para ello. Podría darse el caso de que determinados bienes resultaran físicamente dañados con ocasión de un ciberataque, incluso de que dichos bienes fueran infraestructuras críticas o que determinados sistemas informáticos, de acceso para la población civil, quedasen inutilizados. Sin embargo, ninguno de estos resultados podría calificarse de crimen si no alcanza la gravedad que el propio artículo ejemplifica con la agresión.

De forma idéntica cabe pronunciarse en relación al resto de obligaciones de DIH, que ya han sido objeto de examen en capítulos anteriores. Ya se ha advertido cómo las ciberoperaciones han de guardar la necesaria proporción entre los daños que se causan y el objetivo militar a conseguir. Cualquier desproporción, en estos supuestos, constituirá la violación de esta obligación internacional, pero únicamente las de mayor gravedad, conforme a lo que aquí se expresa, podrán tener la consideración de crimen. En efecto, si a través de un ciberataque se inutilizan las redes de un Ejército en combate y con ello se impide su comunicación interna y/o externa, a semejanza de lo ocurrido en la guerra de Osetia, la desproporción podría acreditarse, en función del objetivo que pretendiera alcanzarse, sin que por ello pueda ser tenida por un crimen de agresión.

En el estudio de la prohibición de la perfidia, en el Capítulo Segundo, hubo ocasión de señalar que la violación de esta obligación internacional consiste en "*matar, herir o capturar a un adversario valiéndose de medios pérfidos*".[699] A esta cualificación inicial, pues, habrá que añadir ahora la que recoge la definición de crimen y únicamente cuando este resultado alcance la relevancia expuesta más arriba, podrá tenerse por tal y, en consecuencia, entender cometida la violación de una norma de *ius cogens*.

Por último, estas mismas consideraciones son aplicables a la obligación de respetar la neutralidad de terceros en caso de conflicto armado.

En segundo lugar, el artículo 19, entiende cometido un crimen internacional, cuando se trate *b) de una violación grave de una obligación internacional de importancia esencial para la salvaguardia del derecho a la libre determinación de los pueblos, como la que prohíbe el establecimiento o el mantenimiento por la fuerza de una dominación colonial*. En este punto, habida cuenta la específica naturaleza del método de combate que se examina, ninguna consideración cabe realizar.

Con carácter previo al examen del apartado tercero del artículo, se hará somera mención al apartado último, que entiende cometido un crimen

699 Artículo 37 del PA I.

internacional como consecuencia, *d) de una violación grave de una obligación internacional de importancia esencial para la salvaguardia y la protección del medio humano, como las que prohíben la contaminación masiva de la atmósfera o de los mares*. Si bien pudiera parecer ajena al objeto de análisis que aquí se trata, no puede dejarse de lado el ejemplo, ya analizado, de la introducción del virus Stuxnet en la central nuclear iraní de Natanz. Es este un supuesto, en el que claramente se pone de manifiesto como un mal uso de una ciberoperación, podría, en su caso, originar un daño *para la salvaguardia y la protección del medio humano, como las que prohíben la contaminación masiva de la atmósfera o de los mares.* En un caso como el que se cita, la realización de un daño en una central nuclear, que supusiera la contaminación del medioambiente, en los términos contenidos en el artículo 19 d), no parecen imposibles. Por lo tanto, hay que tener presente que, a través de una ciberoperación, podría cometerse este crimen internacional y que, en consecuencia, nos encontraríamos ante la violación de una norma imperativa.

Por último, el tercer apartado del referido artículo 19, entiende cometido un crimen internacional a través de c) *de una violación grave y en gran escala de una obligación internacional de importancia esencial para la salvaguardia del ser humano, como las que prohíben la esclavitud, el genocidio y el apartheid.* Es decir, nos encontramos aquí ya con la definición de los crímenes internacionales, sobre los que ejerce su competencia la Corte Penal Internacional y que constituye un criterio de identificación adicional al establecido en el artículo 19 del primer Proyecto, por lo que requerirá un estudio en mayor profundidad.

En esta labor de establecimiento de criterios de identificación de las normas de DIH imperativas, el Estatuto de Roma de la Corte Penal Internacional, en vigor desde el 10 de julio de 2002, se manifiesta como un documento esencial. En consonancia con lo anterior, el estatuto afirma que "*los crímenes más graves de trascendencia para la comunidad internacional en su conjunto no deben quedar sin castig*o" y recuerda que constituye un "*deber de todo Estado ejercer su jurisdicción penal contra los responsables de crímenes internacionale*s"[700]. Así, una de las notas que caracterizan a las normas imperativas es sin duda la "*universality of jurisdiction*

700 Así puede leerse en el Estatuto de la Corte Penal Internacional. Doc. A/CONF.183/9,

over such crimes irrespective of where they were committed, by whom (including Heads of State), against what category of victims, and irrespective of the context of their occurrence (peace or war)[701]".

En concreto, el artículo 8 recoge, expresamente, las conductas que han de considerarse "*Crímenes de guerra*", entendiendo por tales, entre otras, las

> «Infracciones graves de los Convenios de Ginebra de 12 de agosto de 1949, a saber, cualquiera de los siguientes actos contra personas o bienes protegidos por las disposiciones del Convenio de Ginebra pertinente:
>
> i) El homicidio intencional;
>
> *ii) La tortura o los tratos inhumanos, incluidos los experimentos biológicos;*
>
> *iii) El hecho de causar deliberadamente grandes sufrimientos o de atentar* gravemente contra la integridad física o la salud;
>
> iv) La destrucción y la apropiación de bienes, no justificadas por necesidades militares, y efectuadas a gran escala, ilícita y arbitrariamente;
>
> v) El hecho de forzar a un prisionero de guerra o a otra persona protegida a servir en las fuerzas de una Potencia enemiga;
>
> vi) El hecho de privar deliberadamente a un prisionero de guerra o a otra persona protegida de su derecho a ser juzgado legítima e imparcialmente;
>
> vii) La deportación o el traslado ilegal o el confinamiento ilegal;
>
> viii) La toma de rehenes».

Sin que pueda olvidarse, como recuerda EBOE-OSUJI, que la violación de las leyes y usos de la guerra será grave siempre y cuando afecte a personas o bienes protegidos o a valores importantes y cuando se cometa intencionadamente, "*in the sense of intentionally or in reckless disregard of their outcome as endangering protected persons or objects or their breach of important values*"[702].

En consecuencia, de las normas que hasta ahora han venido considerándose el núcleo esencial de DIH, únicamente podrán ser entendidas

---

701 BASSIOUNI, C. *International Crimes: Jus Cogens and Obligatio Erga Omnes*, op. cit.; pp.65 y 66.

702 OSUJI, C. E., Grave breaches' as war crimes: much ado about …'serious violations'?; p.2. Documento disponible en el sitio web: www.icc-cpi.int/NR/rdonlyres/827EE9EC-5095-48C0-AB04-E38686EE9A80/283279/GRAVEBREACHESMUCHADOABOUTSERIOUSVIOLATIONS.pdf . Fecha de consulta, enero 2014.

como norma de *ius cogens*, aquéllas que reúnan los requisitos antedichos y, además, causen uno de los resultados enunciados en este segundo punto, apartado a) del artículo 8 del Estatuto de Roma. Al respecto, REMIRO BROTONS , al abordar la cuestión de la competencia judicial para conocer del crimen de agresión, pone de manifiesto cómo la justicia interna es, en cierto modo, subsidiaria, pues "*solo los jueces del Estado nacional de los presuntos implicados podrían juzgarlos en defecto o como alternativa a tribunales internacionales*" y, a juicio del autor, este criterio sostenido por la CDI demuestra que "*no se puede arrostrar la cuestión de la responsabilidad individual sin considerar previamente la cuestión de la responsabilidad internacional del Estado*".[703]

Por su parte, para el CICR, las violaciones graves de las normas de DIH quedan perfectamente delimitadas en el contenido de los cuatro Convenios de Ginebra, de forma tal que cada uno de ellos recoge cuáles son las violaciones graves contra los mismos que, en consecuencia, han de ser tomadas por crímenes de *ius cogens*[704].

Se trata de examinar, por lo tanto, si la contravención de las normas de DIH que fueron analizadas en el apartado precedente pueden o no incurrir en los resultados previstos en el citado artículo 8[705] y, de esa manera, considerarse como imperativas.

3.1. La necesidad militar.

Así, puesto que ya se ha concluido que una de las normas "inconculcables" del DIH está constituida por la necesidad militar del ataque, a la luz del contenido del artículo 8 del Estatuto de la Corte Penal Internacional, cuando la violación de dicha obligación produzca cualquiera de los resultados

703 REMIRO BROTONS, A. *El crimen de agresión en el estatuto de la CPI revisado: nascetur ridiculus mus*. Estudios de Derecho Internacional y de Derecho europeo en homenaje al Profesor Manuel Pérez González. Tomo I. Aznar Gómez, M., (Coordinador). Tirant lo Blanch. Valencia, 2012; pp. 1115-1130, en particular, p. 1127.

704 Al respecto, véase, CICR, Grave breaches specified in the 1949 Geneva Conventions and in additional Protocol I of 1977, doc. cit.

705 En relación a la distinción entre el acto de agresión y el crimen de agresión, resultan de particular interés las refelxiones reflexiones que ofrece QUESADA ALCALA, C., *La agresión: un crimen "cierto" de futuro "incierto"*, op. cit.; p. 1078.

contenidos en el citado artículo, nos encontraremos ante la violación de una norma imperativa que impedirá la justificación del hecho ilícito.

En este sentido, parece evidente que, como ha quedado argumentado, a través de ejemplos previos, la vida humana es susceptible de ser atacada tanto por métodos de combate cibernéticos, como por métodos de combate convencionales. Por lo tanto, la mención al homicidio internacional, que recoge el artículo 8 del Estatuto, no puede concebirse sin tener en cuenta todos los métodos de combate al alcance de los Estados. En caso contrario, quedaría mermado de contenido el propio Estatuto, pues no hay que olvidar que la tendencia actual de los Estados es proclive a la adquisición de ciberarmas y a la formación de sus Fuerzas Armadas en su manejo. Por ese mismo motivo, una vez más, hay que poner de relieve la importancia de proporcionar la adecuada formación en el manejo de las mismas. Esta formación, como en repetidas ocasiones se ha afirmado, requerirá proporcionar el contenido de todas las cuestiones relativas a DIH, a la luz de las ciberarmas.

De idéntico modo habrá que concluir en relación a la causación deliberada de "*grandes sufrimientos o atentados contra la integridad física o la salud*". También, en este punto, parece factible la comisión cibernética de tales resultados, al igual que los previstos en los subapartados iv) y v) del apartado a) del artículo 8.1 del Estatuto. De hecho, el contenido del apartado iv), viene a confirmar la ausencia de necesidad militar como crimen de guerra, al recoger la "*destrucción y la apropiación de bienes no justificadas por necesidades militares*", sin olvidar que, para merecer tal consideración, las conductas han de ser realizadas "*a gran escala, ilícita y arbitrariamente*". Asimismo, en coherencia con lo anteriormente apuntado, hay que entender incluidos en esos "bienes", los bienes informáticos, que incluirán tanto los materiales como inmateriales, es decir, los equipos y sistemas.

El apartado v) del artículo 8 del Estatuto, por su parte, alude al "*hecho de forzar a un prisionero de guerra o a otra persona protegida a servir en las fuerzas de una Potencia enemiga*". Sin duda, podrá darse el caso de que un prisionero o persona protegida se vea obligado a manejar las ciberarmas en provecho del enemigo. Asimismo, podría darse el caso de que ese forzamiento pudiera realizarse a

través de medios informáticos, cometiendo un cibersecuestro del equipo informático del militar encargado de las ciberoperaciones. Tal y como ocurre en el ámbito penal, puede darse el caso de la captura de un equipo informático a distancia, de manera que, quien se encuentra manejándolo ha de someterse a la voluntad de su "cibersecuestrador" si quiere ver "liberado" su equipo. No parece que pueda descartarse esta posibilidad en el ámbito del conflicto armado y, por lo tanto, cuando ello ocurra, sin que se acredite necesidad militar en ello, nos encontraremos con una ciberoperación ilícita desde el punto de vista del DIH, que impedirá la alegación de cualquiera de las causas de justificación que prevé el Proyecto de artículos, cuando se exija la responsabilidad internacional del Estado infractor. Asimismo, la privación deliberada a *un prisionero de guerra o a otra persona protegida de su derecho a ser juzgado legítima e imparcialmente,* también sería susceptible de ser cometida virtualmente, en el caso de que pudiera interferirse en el sistema de justicia encargado de ello o se destruyeran, por medios cibernéticos, los archivos, pruebas o cualesquiera documentos esenciales, para que dicho proceso se desarrollara con normalidad y justicia.

Sin embargo, en otros de los supuestos previstos en este apartado que se examina parece más complicado que la comisión cibernética llegue a efectuarse. La *tortura o los tratos inhumanos, incluidos los experimentos biológicos,* parecen requerir una intervención física, en algún momento, aunque un ataque cibernético que activara un arma biológica o química sí que podría dar lugar a un experimento biológico. Finalmente, tampoco parece posible desde un punto de vista técnico, la realización de la conducta contemplada en los subapartados finales, que requieren la *deportación o el traslado ilegal o el confinamiento ilegal* y *la toma de rehenes.*

En definitiva, puede afirmarse que la violación de la obligación de DIH, consistente en acreditar esa necesidad militar, puede generar determinados resultados aquí citados. Cuando estos resultados se acrediten y atribuyan a un Estado, en los términos ya vistos, se estará ante la violación de una norma imperativa.

Asimismo, en el Capítulo Segundo del presente trabajo se hizo extensa

referencia a la obligación internacional relativa a la necesidad de observar la distinción entre civiles y combatientes, en el transcurso del combate, sea éste parte de una ciberguerra o bien de un conflicto que también se libra por métodos convencionales. Esta necesidad de distinción, se complica en el ámbito cibernético, tal y como quedó allí apuntado y tal y como también se indicó al abordar la atribución del hecho ilícito. Sin embargo, vuelve aquí a reiterarse la necesidad de aplicar los límites del DIH al cibercombate, sin que la dificultad de prueba pueda justificar la violación de normas de DIH. Como consecuencia de la violación de la norma relativa a esta distinción, podrán producirse, asimismo, los crímenes de guerra que enumera el artículo 8 del Estatuto. El ciberataque que, sin distinción de objetivo, produzca un homicidio intencional, la causación deliberada de grandes sufrimientos o atente gravemente contra la integridad física o la salud; constituirá una grave violación de esta norma de DIH e impedirá justificar dicha conducta. Asimismo, si esa ciberoperación produce la destrucción y la apropiación de bienes, que no se justifique por necesidades militares, a gran escala, ilícita y arbitrariamente, tendrá la misma consideración. Por último, si a través de ese ataque armado virtual se fuerza a un prisionero o a otra persona protegida a servir en las fuerzas de una Potencia enemiga o se privar deliberadamente a un prisionero de guerra o a otra persona protegida de su derecho a ser juzgado legítima e imparcialmente, se dará idéntico resultado. Tal y como antes se exponía, parece que el resto de los crímenes de guerra requieren una intervención del combatiente, más allá de la virtual y, por tal motivo, quedarían al margen de su comisión a través de ciberataques.

3.2. La obligación de distinguir entre civiles y combatientes.

La distinción entre civiles y combatientes del artículo 52 del PA I ha de completarse con la definición de población civil que, de forma excluyente, realiza el PA I, en su artículo 50, al entender que es aquélla que no sea combatiente. En este contexto, pues, hay que retomar el ejemplo que se estudiaba al abordar el contenido de esta obligación de DIH y recordar que, en los ataques sufridos por Estonia en el año 2007, tanto los atacantes como los objetivos de los mismos,

fueron de carácter civil. Esta violación de la obligación internacional podría darse igualmente en una situación de conflicto armado, pues podría darse el caso de que, a través de una ciberoperación, se impidiera el uso del teléfono de emergencias, como ocurrió en Estonia. Si de ello de derivaran los resultados mencionados más arriba y se tratara de una violación grave y a gran escala de esta norma de DIH, nos encontraríamos ante un crimen internacional y ante la violación de una obligación internacional, por la que cabría exigir responsabilidad internacional.

3.3. La obligación de observar la proporcionalidad en el ataque.

En siguiente lugar, hay que abordar la obligación de observar la proporcionalidad en el ciberataque, entendida como se expuso en el correspondiente Capítulo, como la prohibición del uso la fuerza en un grado superior al necesario para el cumplimiento del objetivo militar. La falta de proporción en los daños causados, en relación al objetivo militar, podrá dar lugar, asimismo, a los resultados que aquí se vienen exponiendo. Como se puso de manifiesto, el uso de la red está sujeto a esta prohibición toda vez que nos encontramos ante un método de combate capaz de producir un daño indiscriminado y de afectar, por igual, a instituciones públicas y privadas, así como a civiles.

Por lo tanto, el lanzamiento de un ataque armado, desproporcionado, a través de la red, podrá originar, como ya hemos visto, una serie de consecuencias asimilables a las de un ataque de idénticas características, lanzado a través de un método de combate convencional. Así, cuando Estonia sufrió los ciberataques que han sido repetidamente descritos, podemos concluir que se produjeron ataques desproporcionados, pues muchos de ellos carecían de un objetivo militar y, además, tuvieron entidad suficiente para causar males superfluos o sufrimientos innecesarios. Pues bien, si estos ataques hubieran constituido ciberoperaciones desarrolladas en el transcurso de un conflicto armado, la violación de la obligación de DIH, no hubiera presentado ninguna duda. Si, además, dichos resultados incurrieran en alguno de los apartados del artículo 8

del Estatuto y la violación de la norma de DIH hubiera sido grave y a gran escala, la justificación de dicha violación sería inoperante.

No puede ofrecer duda el hecho de que, a través de un ciberataque armado desproporcionado, podrá cometerse un homicidio internacional, así como la práctica totalidad de los resultados antes enunciados. En los mismos términos que antes se expresaban, una operación cibernética desproporcionada, podrá causar deliberadamente grandes sufrimientos o de atentar gravemente contra la integridad física o la salud[706]; la destrucción y la apropiación de bienes, no justificadas por necesidades militares, y efectuadas a gran escala, ilícita y arbitrariamente; forzar a un prisionero de guerra o a otra persona protegida a servir en las fuerzas de una Potencia enemiga y, por último privar deliberadamente a un prisionero de guerra o a otra persona protegida de su derecho a ser juzgado legítima e imparcialmente.

Asimismo, también aquí parece que el resto de los resultados exigen cierto tipo de intervención física y, por lo tanto, su comisión a través de medios cibernéticos no aparecería tan clara, al menos *a priori*. Sin embargo, ninguna duda puede ofrecer el resto de los crímenes de guerra enunciados en el repetido artículo 8. El lanzamiento de una ciberoperación, sin tener en cuenta la necesidad de la fuerza necesaria para conseguir el objetivo militar, llevaría, como se ha apuntado, a atacar a la población civil o, incluso, a medios militares ajenos al objetivo. Por lo tanto, esa ejecución podría dar lugar, *per se*, a la *destrucción no justificada por necesidades militares, y efectuada a gran escala, ilícita y arbitrariamente* que, en este ámbito, parece el resultado de mayor probabilidad en su comisión, sin olvidar el resto apuntado más arriba. Por lo tanto, puede afirmarse que en relación a la responsabilidad internacional del Estado, las consecuencias de la

706 En relación a la causación de daños físicos, a través de internet, tales como el homicidio internacional o el grave atentado contra la integridad física o la salud, hay que tener en cuenta las últimas novedades científicas que, en este campo, han sido puestas de manifiesto. Así, se ha acreditado la posibilidad de "hackear" sistemas informáticos dedicados a controlar dispositivos como desfibriladores, marcapasos y bombas de insulina, alojadas en el organismo, tal y como ha asegurado el Departamento de Salud de los Estados Unidos. La información al respecto, entre otros sitios, puede consultarse en el propio sitio web del Departamento: www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm. Fecha de consulta, diciembre de 2016.

utilización de este método de combate conllevará la imposibilidad de justificar el hecho ilícito que suponga un crimen de agresión.

3.4. La prohibición de la perfidia.

En este punto, continuando con la sistemática expuesta en el Capítulo Segundo del presente trabajo de tesis, hay que atender a la violación de la obligación de DIH, concerniente a la prohibición de la perfidia. Ya ha sido expuesto cómo, en el desarrollo del cibercombate, resulta de aplicación el artículo 37 del PA I, que establece la prohibición de matar, herir o capturar a un adversario valiéndose de medios pérfidos. Si la perfidia es el abuso de la buena fe de un adversario, a través del que se le da a entender que se tiene derecho a protección, no hay, entonces, objeción a que esta prohibición sea aplicable a las ciberoperaciones. De hecho, ya quedó expuesto cómo, de entre las acciones que el artículo 37 del PA I recoge como ejemplos de perfidia, puede preverse la situación en que éstas sean realizadas por medios cibernéticos.

En este supuesto, la prohibición de valerse de la perfidia aparece doblemente condicionada, pues, para que el hecho ilícito pueda entenderse consumado, es preciso que el cibercombatiente cause alguno de los resultados enumerados en el citado artículo 37. Pues bien, para que dicha ciberoperación pérfid sea tenida, además, por un crimen de guerra, será preciso constatar uno de los resultados contenidos en el artículo 8 del Estatuto. De este modo, podríamos encontramos con el supuesto de que un Estado en combate, valiéndose de la buena fe de un adversario, dándole a entender que se tiene derecho a protección, se produjera la muerte, lesión o captura de un adversario. Por lo tanto, ninguna objeción puede haber a la asunción como posible de un homicidio internacional, valiéndose de medios pérfidos. De hecho, como antes se apuntaba, ha quedado demostrada la posibilidad, desde un punto de vista fáctico, de interferir en los dispositivos que, alojados en el organismo humano tratan ciertas patologías. Por lo tanto, habrá también que aceptar la posibilidad de interferir en dichos sistemas, causando engaño y produciendo un homicidio internacional o un trato inhumano y, en este caso, de forma clara un experimento biológico que, de otro

modo pudiera resultar más complicado de llevar a cabo. Asimismo, podrida darse la producción, aprovechando una actuación pérfida, de perfidia de grandes sufrimientos o de un grave atentado contra la integridad física o la salud.

Por otra parte, esta prohibición, aplicada a los ataques informáticos, implica la ilicitud del ataque a redes pertenecientes a entidades especialmente protegidas, cuando se realice al objeto de transmitir información de contenido militar. Si de ello se derivara, pues, alguno de los resultados anteriormente analizados, también nos encontraríamos ante la violación de una norma imperativa.

3.5. La obligación de respetar la neutralidad de terceros Estados.

Por último, como se exponía en el capítulo Segundo, la neutralidad es la situación jurídica y política de un Estado que permanece al margen de un conflicto armado y se abstiene de ayudar a cualquiera de los beligerantes. El respeto a la neutralidad de terceros constituye, pues, otros de los principios cardinales del DIH que ha de verse respetado en todo momento, con independencia del método de combate que se utilice por los Estados en conflicto.

El contenido de esta norma obliga a un análisis en estrecha relación con el resto de normas de DIH, pues, evidentemente, esta neutralidad exigirá un claro discernimiento de la titularidad y dominio de las redes, equipos y sistemas informáticos que pretendan ser usados por las partes en conflicto. Todo ello, sin perjuicio, nuevamente, de los habituales problemas de atribución que se vienen poniendo de manifiesto, a lo largo del presente trabajo. En cualquier caso, la comisión de cualquiera de los crímenes de guerra previstos en el artículo 8 del Estatuto, violando la obligación de DIH de respetar la neutralidad de terceros, conllevará la violación de una norma de *ius cogens*, cuando la violación sea grave y a gran escala. En este supuesto, el uso de un sistema, equipo o red de un tercero neutral podrá causar un homicidio internacional. Puede aquí ser retomado el ejemplo de una ciberoperación que se lance contra una persona especialmente protegida por el pertinente Convenio de Ginebra y que conlleve su muerte. Dicha operación cibernética podría necesitar del uso de la red de un tercer Estado o de

la utilización de un medio disponible sólo por ese tercer Estado que se muestra neutral. De este modo, si violando dicha neutralidad se consumara el citado hecho ilícito, también nos encontraríamos ante la violación de una norma imperativa de DIH y, por lo tanto, ante la imposibilidad de justificar dicha conducta por el Estado infractor.

Asimismo, la violación de la neutralidad podría favorecer la producción de una ciberoperación que, a su vez, permitiera inflingir tratos inhumanos o experimentos biológicos, en los mismos términos que se presentaban al hablar de la prohibición de la perfidia. De igual manera, en el transcurso de una ciberguerra o al lanzar una ciberoperación, valiéndose de redes, equipos, sistemas o cualquier medio perteneciente a un tercero neutral, podría darse un resultado consistente en la causación de grandes sufrimientos o el grave atentado contra la integridad física o la salud. Tampoco parece impensable que, violando la obligación de neutralidad, puedan producirse el resto de resultados recogidos en el artículo 8, a salvo, claro está, de aquéllos que, como ocurría en los supuestos anteriores requieran, en un momento u otro, una intervención física por parte del combatiente y no exclusivamente una ciberoperación. De este modo, no puede descartarse la destrucción y la apropiación de bienes que sin justificación militar, se produzcan, a gran escala, ilícita y arbitrariamente, como consecuencia de un ciberataque armado, lanzado a través de un Estado neutral. Por último y, en los términos anteriormente expuestos, cabría considerar la posibilidad de que una ciberoperación pudiera utilizarse para privar deliberadamente a un prisionero de guerra o a otra persona protegida de su derecho a ser juzgado legítima e imparcialmente. En consecuencia, todas estas situaciones comportarían la violación de una norma de DIH de *ius cogens* y, por ende, la imposibilidad de justificación, desde el punto de vista de la responsabilidad internacional.

La consideración de determinadas normas de DIH como normas imperativas es, al margen de aparecer como lógica tras el examen del precepto, además, necesaria, habida cuenta las actuales circunstancias que condicionan el desarrollo de los conflictos armados. La extensión de los conflictos híbridos, la participación de agentes no estatales en el conflicto armado, la confusión entre los

actos de combate y de terrorismo hacen de los conflictos armados, una situación fáctica, de calificación jurídica, en ocasiones, dudosa, de la que pueden beneficiarse quienes pretender evadirse del cumplimiento de las normas que lo rigen. Por resulta de suma importancia que determinadas normas de DIH tengan consideración de *ius cogens*.

3.6. Otras violaciones graves.

Por otra parte, no puede olvidarse que en el citado Estatuto de Roma, en el subapartado b) del artículo 8, se cita "*otras violaciones graves*" que, cometidas en el transcurso de un conflicto armado internacional, también constituyen crímenes de guerra. Entre ellas y sin ánimo de exhaustividad, pueden encontrase la práctica totalidad de las normas que, en Capítulos precedentes, se han examinado y valorado como esenciales, en la configuración del contenido del DIH. Así, este apartado b), incluye los ataques contra la población civil que no participe directamente en las hostilidades, los ataques contra bienes civiles, los que se produzcan contra bienes que no sean objetivos militares, el uso indebido la bandera blanca, de la bandera nacional o de las insignias militares, del uniforme del enemigo o de las Naciones Unidas, así como de los emblemas distintivos de los Convenios de Ginebra que cause la muerte o lesiones graves. Es decir, en la mayoría de los supuestos en que se produzca una violación de una norma de DIH, el Estado trasgresor estará infringiendo una norma imperativa.

Como pone de relieve MEDLONG, los Convenios de Ginebra parecen establecer una dicotomía entre las "*graves violaciones*" de sus preceptos y los "*actos contrarios a las previsiones de la Convención correspondiente*[707], pese a que, en un principio, otros autores afirmen la existencia de normas que, comúnmente, son aceptadas como imperativas, sin controversia.[708]

La importancia de la cuestión apuntada radica en el hecho de que nos

707 MEDLONG, J. *All Other Breaches: State Practice and the Geneva Conventions' Nebulous Class of Less Discussed Prohibitions*.Michigan Journal of International Law, vol. 34, issue 4; pp. 829-856, en particular, pp. 829-830.

708 BRILMAYER, L. y TESFALIDET, I. Y., "*The norms most commonly cited as falling into this category are: the prohibitions of genocide, piracy, slaving and slavery, torture, and wars of aggression or for territorial expansion.*", en *Third State Obligations And The Enforcement Of International Law*. International Law And Politics, 2011, vol. 44; pp. 2-56, en particular, p. 21.

hallamos, en este punto, en el análisis de la relación jurídica que surge como consecuencia de la violación de una obligación internacional. Es decir, si la responsabilidad internacional no puede entenderse como una mera consecuencia resultante de unos hechos previos, sino como una relación jurídica sustantiva que nace de la violación de una obligación internacional. Cuál sea dicha relación jurídica dependerá, enteramente, de la naturaleza de la norma violada que la hace surgir.

4. CONSECUENCIAS DE LA VIOLACIÓN DE UNA NORMA IMPERATIVA.

De la comisión del hecho ilícito internacional, se derivarán las consecuencias que han sido apuntadas, en el examen del concreto contenido de las obligaciones de DIH que se analizaban en el Capítulo segundo.

Sin embargo, en este punto, hay que hacer constar que las consecuencias relacionadas con la transgresión de una norma imperativa, presentan ciertos caracteres propios. En primer lugar, frente a dicha violación, al Estado transgresor se le podrá exigir responsabilidad internacional, pues el primero de los efectos contenidos en el Proyecto es la imposibilidad de justificar este hecho ilícito. Es decir, ninguna de las causa de exclusión de la ilicitud que se verán posteriormente podrá entrar en juego cuando se haya cometido al violación de una norma imperativa.

Puede afirmarse, siguiendo a PÉREZ GONZÁLEZ que se trata de hechos que "*por contradecir ciertas reglas básicas de la convivencia internacional y ciertas exigencias éticas de carácter esencial, pueden dar lugar a un régimen de responsabilidad internacional particularmente severo*[709]". Son pues, normas de carácter universal[710] y cuya existencia persigue una finalidad que podría calificarse como superior a los fines perseguidos por el resto de normas internacionales.

Además, hay que tener presente la posibilidad de que dicha

709PEREZ GONZALEZ, M. *La responsabilidad internacional,* op. cit.; p. 881.

710 Según CEBADA ROMERO, el hecho de que las circunstancias excluyentes de la ilicitud no operen en relación con la violación de normas imperativas, refuerza también su carácter inderogable. CEBADA ROMERO, A. *Los conceptos de obligación erga omnes, ius cogens y violación grave a la luz del nuevo proyecto de la CDI sobre responsabilidad de los Estados por hechos ilícitos*, op. cit.; p.4.

responsabilidad sea exigida por parte de la Comunidad Internacional en su conjunto, pues no podemos olvidar que éste es uno de los rasgos definitorios de dichas normas de *ius cogens*.

Además de lo anterior, hay que hacer mención al artículo 41 del Proyecto de responsabilidad internacional que prevé que cuando una norma de *ius cogens* es objeto de violación, los Estados deben de cooperar para poner fin, por medios lícitos, a la violación grave de la misma; en segundo lugar, se impone asimismo a los Estados la obligación de no reconocer, como lícita, una situación creada por una violación grave de una norma de *ius cogens* y, por último, no deben prestar ayuda o asistencia al Estado para mantener dicha situación y otras consecuencias que la violación grave pueda generar según el Derecho internacional.

Sin embargo, estas específicas consecuencias no se producen de forma alternativa sino, antes bien, "*sin perjuicio de las demás consecuencias jurídicas básicas, que nacen por los hechos internacionalmente ilícitos*[711]".

No obstante, si se examina cada una de las consecuencias enumeradas, se evidencia la falta de concreción que el Proyecto ofrece en relación a la puesta en práctica de las mismas. El mismo Comentario al Proyecto, así lo pone de relieve, al afirmar que no aparecen descritas en el citado Proyecto qué medidas deben adoptar los Estados para poner fin a las violaciones graves, en el sentido del artículo 40[712].

En relación al deber de cooperación, tendrá que ser exigido a los Estados, independientemente de que resulten o no afectados por la violación grave ni de su participación en el hecho ilícito, pues no puede obviarse que nos hallamos ante obligaciones que involucran a la Comunidad Internacional en su conjunto. Así ha sido entendido también por la CIJ, que en la Opinión Consultiva, emitida con motivo de la construcción de un muro en los territorios ocupados de Palestina, indicó que todos los Estados tiene la obligación de poner fin al hecho

711 QUISPE REMÓN, F. *Las normas de ius cogens: ausencia de catálogo,* op. cit.; pp.178 y 179.
712 Así lo han puesto también de manifiesto BRILMAYER, L. y TESFALIDET, I. Y., *Third State obligations and the enforcement of International Law*, op. cit.; p. 21.

ilícito objeto de la consulta[713]:

> "It is also for all States, while respecting the United Nations Charter and international law, to see to it that any impediment, resulting from the construction of the wall, to the exercise by the Palestinian people of its rights to self-determination is brought to an end".

Las consecuencias de que una norma sea reconocida como imperativa no se limitan a la posibilidad de que los Estados puedan denunciar su violación, con independencia de que hayan sido o no perjudicados por la misma, sino que abarca a las relaciones jurídicas que nacen de dicha infracción. De este modo, todo Estado, por el hecho de pertenecer a la Comunidad internacional, viene obligado a adoptar las medidas necesarias para poner fin a las violaciones graves. A mayor abundamiento si se entiende que la Comunidad Internacional no se limita al conjunto de Estados, sino que abarca a todo sujeto de Derecho Internacional, esta exigencia también vendría referida a estos sujetos. La creciente importancia de los agentes actuantes en el ámbito internacional favorece la adopción de dicha tesis, ya que, por una parte, se conseguiría no limitar la responsabilidad internacional a solo un ámbito de los sujetos de Derecho Internacional, es decir, los Estados, ni se impediría que quienes gozan de personalidad jurídica y derechos asumieran, al mismo tiempo, sus obligaciones.

De esta manera, en el caso que aquí se examina, podría darse el supuesto de la violación de una norma de *ius cogens*, de DIH, como por ejemplo, destrucción y la apropiación no justificadas por necesidades militares, y efectuadas a gran escala, ilícita y arbitrariamente de bienes, del artículo 8.1 a) iv) del Estatuto de Roma. En este caso, podría ocurrir que terceros Estados, no responsables de dicha infracción ni perjudicados por la misma, estuvieran en posesión de medios técnicos que permitieran poner fin a un ciberataque contra objetivos civiles. Si las capacidades militares son heterogéneas entre los Estados, aun lo son más cuando se trata de medios cibernéticos, pues el nivel de desarrollo de las medidas llamadas de ciberdefensa dependerá de múltiples factores, de

713Legal Consequences cf the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I. C. J. Reports 2004; par.189.

manera que la cooperación internacional podrá resultar crucial para poner fin a la violación de esta norma internacional, sin perjuicio del ejercicio de la legítima defensa que, en su modalidad colectiva y, por los mismos motivos, resultará determinante, como se verá posteriormente.

En cualquier caso, como enuncia el Comentario al Proyecto, ante las violaciones graves, todos los Estados deben realizar un esfuerzo conjunto y coordinado para contrarrestar los efectos de esas violaciones.

En segundo lugar, se contempla la obligación de no reconocimiento colectivo por la Comunidad Internacional de la legitimidad de situaciones directamente resultantes de violaciones graves, en el sentido del artículo 40. En el hipotético caso, antes enunciado, de que se produjera la privación deliberada a un prisionero de guerra o a otra persona protegida, de su derecho a ser juzgado legítima e imparcialmente, el acatamiento de la decisión judicial por la Comunidad Internacional, en su conjunto, resultaría contrario al cumplimiento de esta obligación, pues, como afirma el Comentario al Proyecto[714], ningún Estado reconocerá como lícita una situación creada por una violación grave y esta obligación se aplica a todos los Estados, incluido el Estado responsable.

Por último, en el párrafo 2 del mismo artículo se prohíbe a los Estados prestar ayuda o asistencia para mantener una situación creada por una violación grave en el sentido del artículo 40. La CDI, en su Comentario al Proyecto, aclara que esta prohibición se extiende más allá de las medidas de apoyo o asistencia que se contemplan en el artículo 16, y que ya han sido objeto de estudio en otra parte del presente trabajo. En este caso se trata de la asistencia prestada *a posteriori* al Estado responsable, con el objetivo de ayudar a que se mantenga una situación contraria a una obligación oponible a todos los Estados, en el sentido de hacer ilegal *erga omnes* una situación que se mantiene en violación del Derecho Internacional. En el hipotético ejemplo que aquí se presenta, la ayuda que un tercer Estado u otro miembro de la Comunidad Internacional pudiera prestar para la ejecución de penas impuestas tras la celebración de un proceso en el que deliberadamente se hubiera omitido el derecho a ser juzgado legítima e imparcialmente, entraría dentro de esta prohibición. Así, la

714 Comentario 4) al artículo 41 del Proyecto.

aplicación de cualquier Convenio de asistencia mutua que pudiera preexistir a la celebración de tal proceso estaría incurriendo en la contravención de esta obligación.

En consecuencia, puede concluirse que una violación grave en el sentido del artículo 40 dará lugar a una obligación, para el Estado responsable, de cesar el hecho ilícito, seguir el cumplimiento de su obligación y, en caso apropiado, dar garantías y seguridades de no repetición. Asimismo, de manera adicional y no disyuntiva, se exige al mismo Estado que cumpla con el deber de reparar, de conformidad con lo dispuesto en el Proyecto para el surgimiento de las relaciones jurídicas propias de la responsabilidad internacional. Por último, con CEBADA ROMERO, puede afirmarse la diferencia entre la violación de una norma imperativa y la comisión de un ilícito común, varía, esencialmente, en "*el alcance de las obligaciones internacionales a cargo del Estado responsable que, en el primer caso, existen frente a toda la Comunidad internacional*"[715].

En cualquier caso, "un Estado que comete un crimen de agresión, un crimen de guerra, un crimen contra la humanidad o un genocidio viola las normas del ius cogens , y que por consiguiente no cabe justificación legal alguna[716]."

5. CONCLUSIONES AL CAPÍTULO CUARTO.

PRIMERA: Atendiendo a los caracteres del *ius cogens*, la utilización de un ciberataque como método de combate prohibido por el DIH puede constituir la violación de una norma imperativa y, en consecuencia, un ciberataque prohibido por el DIH no justificará el hecho ilícito cometido.

Así se deduce del estudio de las normas imperativas cuya existencia se establece en la legalidad internacional y ha sido reconocida por la Jurisprudencia. Las teorías negacionistas de la existencia de las normas imperativas han de abandonarse, a la luz de la definición ofrecida por el artículo 53 de la Convención

715 CEBADA ROMERO A. *Los conceptos de obligación erga omnes, ius cogens y violación grave a la luz del nuevo proyecto de la CDI sobre responsabilidad de los Estados por hechos ilícitos*, op.cit; p.11.

716 De este modo concluyen GALAND, R.y DELOOZ, F. en "El artículo 31, párrafo 1, apartado c) del Estatuto de la Corte Penal Internacional: ¿cuestionamiento de los logros del derecho internacional humanitario?", de 30 de junio de 2001. Revista Internacional de la Cruz Roja. Informe de un estudio realizado por la Comisión consultiva de derecho internacional humanitario de la Cruz Roja de Bélgica, Comunidad francófona, bajo la presidencia del profesor Éric David, Universidad libre de Bruselas. Disponible en el sitio web: https://www.icrc.org/spa/resources/documents/misc/5tdpq2.htm.

de Viena sobre los Tratados. Esta definición, por otra, parte, permite considerar que las normas de DIH, objeto de atención, tienen naturaleza de *ius cogens*, pues reúnen los caracteres enumerados en dicho artículo.

No puede negarse que, al examinar las limitaciones que el DIH impone a la utilización de los métodos de combate nos encontramos ante normas imperativas, pues dichos límites constituyen normas universales, imperativas y protectoras de bienes jurídicos superiores. Atendiendo al Proyecto de artículos sobre responsabilidad internacional de los Estados, puede afirmarse que la violación flagrante y sistemática de una norma de DIH constituye la violación grave de una norma imperativa y, por lo tanto, la utilización de un ciberataque, como método de combate, que incurra en tales condiciones, se tendrá por la violación grave de una norma imperativa.

Como hasta ahora se ha expuesto, el uso del método de combate cibernético no difiere, en relación al resto de métodos, a la hora de exigir el cumplimiento de las normas de DIH. Las diferencias que pudieran hallarse entre el uso de un método y otro vendrán dadas por los condicionantes prácticos. En consecuencia, en la medida en que los ciberataques transgredan, de forma flagrante y sistemática, los límites impuestos por el DIH, constituirán la violación de una norma imperativa. Así, por ejemplo, un ciberataque lanzado durante el conflicto y que impida las comunicaciones civiles de forma sistemática, se tendrá que calificar como un hecho ilícito que desobedece las normas de *ius cogens*, pues, de forma flagrante, se estaría violando la norma que obliga a la distinción entre objetivos civiles y militares. Lo mismo cabría decir de la operación cibernética que, por ejemplo, desvelara datos relativos al personal militar, ajenos a su actividad en las Fuerzas Armadas, pues se daría, de forma flagrante, una operación carente de necesidad militar. En ambos supuestos, la violación sistemática resultará de sencilla comisión a través de métodos informáticos, pues ya se ha expuesto, en el capítulo segundo, al tratar el hecho ilícito continuado, cómo a través de un ciberataque, los efectos que se persiguen pueden darse prolongadamente en el tiempo.

SEGUNDA: Algunas de las normas de DIH que calificarían un ciberataque como método de combate prohibido podrán ser consideradas como normas de *ius cogens,* atendiendo a los caracteres y criterios de identificación de las normas imperativas.

En consecuencia, vuelven a ponerse de manifiesto las consideraciones, hasta ahora realizadas, en relación al concepto de ciberataque armado. De nuevo, será determinante al atribuir el carácter imperativo de la norma de DIH. Las normas imperativas son identificadas a través del criterio de atribución de competencia a la CPI de los hechos ilícitos recogidos en el artículo 8 del Estatuto de Roma. De este modo, el citado artículo considera que son crímenes de guerra, las "*Infracciones graves de los Convenios de Ginebra de 12 de agosto de 1949*". Esas infracciones graves, es decir, flagrantes y sistemáticas, únicamente podrán cometerse a través de ciberataques que constituyan un ataque armado, en los términos que aquí se vienen defendiendo.

TERCERA: El carácter imperativo de algunas de las normas de DIH que califican un ciberataque como método de combate prohibido tendrán como consecuencia la puesta en marcha del mecanismo de responsabilidad internacional del Estado.

El reconocimiento del carácter imperativo de algunas de las normas de DIH aplicables al combate, supone un paso más en relación al cumplimiento de las mismas, pues su violación podrá denunciarse por la Comunidad Internacional en su conjunto. Como se exponía con motivo de las medidas de reparación de la responsabilidad internacional, la violación de una norma de DIH deberá tender, principalmente, a la cesación en la misma y a la persecución del Estad responsable del hecho ilícito. Es decir, el cumplimiento de las normas relativas al combate debe imponerse a los Estados a través de todos los medios que, conforme a la legalidad internacional estén a disposición de los Estados y de la Comunidad Internacional.

Asimismo, se pone en evidencia, nuevamente, la necesidad de asumir un criterio restrictivo a la hora de atribuir el hecho ilícito al Estado. Las consecuencias de la

comisión de una violación grave, utilizando este método de combate por parte de cibervoluntarios no pueden recaer en un Estado, si no se prueba fehacientemente un vínculo entre aquéllos y éste, en las condiciones expresadas en el Capítulo precedente.

En consecuencia, la comisión de cualquiera de los hechos enumerados en el artículo 8 del Estatuto impedirá que el ciberataque prohibido encuentre su justificación en ninguna de las causas expresadas en el Proyecto.

CAPÍTULO QUINTO. LA LEGÍTIMA DEFENSA Y OTRAS CAUSAS QUE EXCLUYEN LA ILICITUD DE LOS CIBERATAQUES QUE CONTRAVENGAN EL DIH.

1. INTRODUCCIÓN.

Una vez delimitado en el capítulo precedente, el ámbito del DIH que puede ser considerado *ius gogens* y, por lo tanto, encuadrable en el artículo 26 del Proyecto, han de analizarse las causas o circunstancias que podrán excluir la ilicitud del hecho.

Estas causas, previstas en el Capítulo V del Proyecto de artículos, tutelan una serie de intereses superiores a los vulnerados por el hecho ilícito y permiten, así, justificar la conducta del Estado infractor. El referido Capítulo del Proyecto recoge de este modo, un catálogo de causas tasadas expresivas de las circunstancias, casi siempre excepcionales que impiden el nacimicento de la relación jurídica de responsabilidad internacional.

Nuevamente, la intervención del elemento cibernético condicionará determinadas situaciones que habrán de reinterpretarse conforme a esta nueva modalidad de combate, sin abandonar, en modo alguno, la interpretación más acorde con la literalidad del Proyecto. En este estudio resultará de vital importancia, asimismo, acudir a los dictámenes de la Jurisprudencia internacional, así como al método teórico-práctico hasta ahora empleado, para discernir la correcta aplicabilidad de las citadas causas de justificación.

En definitiva, se tratará de determinar en qué supuestos la ilicitud del hecho que viola una norma de DIH, relativa, por ejemplo, a la necesidad militar del ciberataque o a la obligación de distinguir entre objetivos civiles y militares puede verse justificada.

En esta labor, se atenderá a cada una de las causas enumeradas en el Capítulo V del Proyecto, sin olvidar la naturaleza imperativa de las normas de DIH que haya sido admitida en el capítulo previo. El estudio de estas circunstancias, sin embargo, impone una sistemática que se aparta de la seguida en el Proyecto, pues el ámbito bélico en el que el hecho ilícito objeto de estudio,

se manifiesta, obliga a atender, con carácter preeminente la legítima defensa, para pasar, después a abordar el resto de circunstancias.

Por otra parte, esta causa merece especial atención por cuanto, además, el ejercicio de la legítima defensa constituye una de las escasísimas circunstancias que justifican el uso de la fuerza, conforme a la legalidad internacional.

Por otra parte, no puede dejarse al margen la evolución conceptual en torno a esta cuestión, sufrida como consecuencia de los atentados ocurridos en los Estados Unidos el 11 de septiembre de 2001. En este sentido, hay que poner de relieve que, ciertamente, el concepto de legítima defensa ha exigido, tradicionalmente, de la interpretación doctrinal y jurisprudencial pues, los requisitos que la conforman han tenido que ser delimitados de acuerdo con la evolución de las formas de agresión ilícita. Sin embargo, la construcción por parte de la doctrina, de nuevos conceptos tales como la "legítima defensa anticipada" o "preventiva", requieren un análisis detenido de esta causa de justificación de forma independiente de las demás ya vistas.

En este estudio, se partirá de las conclusiones alcanzadas a lo largo del presente trabajo, pues difícilmente puede abordarse el análisis de la legítima defensa obviando el concepto de ataque armado y, por lo tanto, sin acudir de nuevo a lo expuesto al comienzo de primer capítulo en torno a dicha cuestión. La delimitación del ataque armado cibernético, vuelve a ser determinante para concretar si, en efecto, nos encontramos ante la posibilidad de ejercer esta legítima defensa. Por lo tanto, habrá que examinar si nos encontramos ante un nuevo modo de ejercer este derecho, en función del ataque cibernético sufrido y, también, en qué momentos resulta condicionante este elemento cibernético, bien a la hora de dirigir la agresión ilegítima bien de responder en legítima defensa.

Por otra parte, como consecuencia de las preliminares consideraciones señaladas, resulta obligada la referencia al momento en que la defensa pueda ser ejercida para entender que la misma es legítima. La exigencia de que la respuesta sea coetánea al ataque ha sido puesta en cuestión, de forma tan contundente por la doctrina internacionalista, que una nueva reflexión sobre este aspecto parece oportuna. Este análisis parece aún más necesario si tenemos en cuenta que

abordamos el estudio de un arma que puede variar de manera sustancial el desarrollo del combate y la respuesta a los ataques armados. La detención del ataque será crucial en estos supuestos y la completa desvirtualización del mismo, tendrá que ser el objetivo a alcanzar.

En cualquier caso, tampoco en este supuesto quedará legitimada la respuesta que se ofrezca cometiendo la violación de una norma de DIH imperativa, en los términos vistos en el capítulo precedente.

En el estudio de la leítima defensa, por último, parece obligado atender a los supuestos de legítima defensa individual y colectiva, a la luz del papel que juega la OTAN, en este específico ámbito. Si bien los supuestos de legítima defensa colectiva no requieren un especial detenimiento en su estudio, sí es cierto que la alusión a esta Organización Internacional se hace obligada, por cuanto es evidente que las capacidades de los Estados en materia de ciberdefensa, son tan dispares que el recurso a la defensa colectiva militar, parece una respuesta probable.

Seguidamente se tendrán en cuenta el resto de las causas que, a la luz del Capítulo V del Proyecto de artículos pueden justificar el hecho ilícito del Estado infractor, impidiendo, así, la exigencia de responsabilidad internacional. En esta segunda parte del presente capítulo se atenderá, en primer lugar, a la posibilidad de que el Estado infractor justifique su conducta en virtud del consentimiento prestado por el Estado lesionado. Para ello habrá que tener presente que el Estado en conflicto podrá ser víctima de la violación de obligaciones internacionales de muy variada naturaleza. En consecuencia, se hará necesario examinar los requisitos del válido consentimiento del Estado, así como los sujetos que tengan la legitimidad suficiente para prestarlo. Sin embargo, acudiendo al ámbito específico que aquí se expone, estas cuestiones deberán, finamente recalar en el análisis de la violación de obligaciones de DIH en los términos previamente expuestos. En este punto, las cuestiones de atribución objeto de estudio en el capítulo tercero volverán a cobrar importancia.

De nuevo, pues, vuelve a girar la cuestión de la responsabilidad internacional en torno al eje que constituye la atribución de la conducta que, pese

a no precisar ningún examen adicional, no podrá dejarse completamente al margen, en la exposición de las causas de justificación.

En segundo lugar, el Proyecto presenta las contramedidas, como modo de justificar la violación de una obligación internacional. En este supuesto, habrá que comprobar si resulta legítima la respuesta a la violación de una obligación de DIH, a través de dichas contramedidas y, en tal caso, en qué condiciones puede alcanzarse dicha licitud. El específico ámbito que aquí se estudia obliga a deslindar lo que podrían considerarse dos caras de la misma moneda: las contramedidas y las represalias bélicas. La naturaleza imperativa de determinadas normas de DIH, vista en el primer epígrafe condiciona el análisis del resto de las causas de justificación y, aun en mayor medida, de las contramedidas. Como en el caso previo, será preciso tener presentes todas las circunstancias de hecho en que puede encontrase un Estado que libra un conflicto armado. Así, habrá que estudiar si de la violación de una obligación internacional, en ese contexto, se deriva la posibilidad de adoptar dichas contramedidas o, por el contrario, nos encontramos ante la excepción prevista en el Proyecto, relativa a las represalias. Para ello, además de acudir, nuevamente, al análisis previamente realizado en relación a las normas de *ius cogens*, será necesario estudiar el específico régimen relativo a las represalias bélicas, previsto en la Compilación de DIH Consuetudinario.

En tercer lugar, además del consentimiento emitido por el Estado y la adopción de contramedidas, en virtud del texto del Proyecto, la actuación del Estado podrá entenderse lícita si la misma, aun violando una obligación internacional, responde a una situación de fuerza mayor. Vuelve a plantearse, en este caso, la necesidad de relacionar conceptos que, pese a haber sido sobradamente analizados por la doctrina interna e internacionalista, así como por la Jurisprudencia, requieren ahora una nueva comprensión, a la luz de la guerra cibernética. Es decir, se trata de evaluar si un ciberataque lanzado durante el combate puede contravenir las normas de DIH, como consecuencia de una fuerza mayor que impida su detención.

Seguidamente, tendrá que examinarse si la situación de peligro extremo o

de estado de necesidad puede, asimismo, justificar la violación de una norma de DIH. Ambas circunstancias cuentan con la suficiente consolidación, en relación a los requisitos exigibles para su acreditación. No obstante, qué haya de entenderse por peligro extremo o por estado de necesidad, en una situación tal, que justifique el hecho ilícito cometido por un ciberataque, constituye un nuevo reto en la delimitación de estas circunstancias. Tal y como se adelantaba, será oportuno hacer mención, nuevamente, a la acreditación de la atribución de la conducta pues, en ambos casos, la actuación previa del Estado infractor que pretende justificarse, resulta determinante para admitir o no dicha justificación.

2. ESPECIAL CONSIDERACIÓN A LA LEGÍTIMA DEFENSA, COMO CAUSA DE JUSTIFICACIÓN DEL HECHO ILÍCITO INTERNACIONAL.

El artículo 21 del Proyecto establece que no puede exigirse responsabilidad internacional del Estado si el hecho ilícito "*constituye una medida lícita de legítima defensa, tomada de conformidad con la Carta de Naciones Unidas*". Esta exención de responsabilidad por el hecho ilícito internacional, ha de contemplarse como una medida coherente con la regulación del uso de la fuerza en la Carta de Naciones Unidas pues, en caso contrario, anularía la efectividad del ejercicio de la legítima defensa, tal y como se recoge en su artículo 51[717]. Al mismo tiempo, ha resultado tan esencial al comportamiento de los Estados, en sus relaciones internacionales, que la legítima defensa fue incluida como causa de exención de la responsabilidad internacional ya por el Comité Preparatorio de la Conferencia de La Haya de 1930[718]. En relación con las normas aplicables al combate, la aplicación de la legítima defensa, en el ámbito del DIH, también fue

717 En el mismo se estipula: "*Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales*". Artículo 51 de la Carta de Naciones Unidas.

718 Así se refleja en el Comentario al Proyecto, que afirma que el Comité Preparatorio, entre sus Bases de Discusión, enumeró dos "*Circunstancias en que el Estado puede declinar su responsabilidad, a saber, la legítima defensa y las represalias*". Comentarios al Proyecto de artículos de responsabilidad internacional.

objeto de discusión, desembocando en la indiscutida admisión de la misma, en la actualidad[719].

En el ámbito que nos ocupa, esta causa de exención resulta, asimismo, coherente con lo expuesto hasta ahora pues, si hemos concluido que un ciberataque puede revestir la naturaleza y gravedad de un ataque armado, la legítima defensa frente al mismo ha de verse como consustancial a la agresión[720]. Por lo tanto, la defensa del Estado será legítima, en primer lugar, si se dirige a repeler una agresión, en el sentido recogido en la Resolución 3314, objeto de examen en el Capítulo Primero del presente trabajo, al exponer el análisis conceptual de los ciberataques. Únicamente cuando el hecho ilícito del Estado infractor revista las condiciones expuestas en la citada Parte del trabajo, nos encontraremos ciertamente ante una agresión, que justifique la respuesta en legítima defensa.

Sin embargo, no puede olvidarse que, como en los supuestos anteriores, cabrá la posibilidad de que un hecho ilícito no constituya un ataque armado. Cuando de ello se derive la puesta en peligro para determinadas personas podremos encontrarnos, no ante la necesidad de ejercer la legítima defensa, sino de invocar por parte del Estado agredido, las circunstancias de peligro inminente

719 DOSWALD BECK aclara que si bien dicha aplicabilidad fue discutida en la preparación del Manual de San Remo sobre el derecho internacional aplicable a los conflictos armados en el mar, no obstante, la CIJ, en su Opinión Consultiva en relación al empleo de las armas nucleares aclaró la cuestión, y, en palabras del autor: "*En su análisis general del derecho, la Corte, en los párrafos 41 y 42 de su Opinión, se declara de acuerdo con la opinión según la cual se aplican las restricciones de ambos ámbitos jurídicos: "La sumisión del ejercicio del derecho de legítima defensa a las condiciones de necesidad y proporcionalidad es una norma de derecho internacional consuetudinario ... Pero, al mismo tiempo, el empleo de una fuerza proporcional con arreglo al derecho de legítima defensa también debe, para ser lícita, cumplir con las exigencias del derecho aplicable a los conflictos armados entre los que cabe mencionar, en particular, los principios y las normas de derecho humanitario. (…) [*La*] doctrina, según la cual, en circunstancias de peligro extremo, se pueden dejar de aplicar las normas de derecho humanitario para hacer frente al peligro, fue rechazada por el Tribunal de Nuremberg en los casos de Peleus, Milch y Krupp*.". DOSWALD-BECK, L., *El derecho internacional humanitario y la Opinión consultiva de la Corte Internacional de Justicia sobre la licitud de la amenaza o del empleo de armas nucleares*. 31 de enero de 1997. Revista Internacional de la Cruz Roja. Documento disponible en el sitio web: https://www.icrc.org/spa/resources/documents/misc/5tdldg.htm. Fecha de consulta, marzo de 2013.

720 Así lo entiende la doctrina internacionalista que no halla diferencias, en este aspecto entre el espacio físico y el virtual en relación al ejercicio de la soberanía nacional "*In cyberspace as in other spaces, states remain sovereign, with rights fully recognized in the* U.N. *Charter.*" LOTRIONTE, C., Sovereignty and self-defense in cyber space. Emory International Law Review, vol. 26; pp. 826-919, en particular, p. 829.

o de estado de necesidad[721].

2.1. La necesidad de la defensa y el momento de ejercerla.

La configuración del ejercicio de la legítima defensa obliga a reconsiderar los conceptos y requisitos, tradicionalmente estudiados al tratar el ataque armado, perpetrado por métodos de combate tradicionales. El modo en que han de ser interpretados, los requisitos de la respuesta ante una agresión ilegítima, en el contexto cibernético, puede poner de relieve una laguna que nunca será deseable pues, no cabe duda de que la respuesta que se ofrezca, en legítima defensa, ha de verse sometida incuestionablemente a unos limites jurídicos claros[722].

En el caso de los ciberataques, una parte de la doctrina internacionalista ha llegado a plantear si, realmente, su empleo constituye uso de la fuerza y, por lo tanto, genera el consiguiente derecho a la legítima defensa[723]. Sin embargo, esta cuestión no puede ofrecer dudas a la luz del análisis conceptual que se ha realizado de los ciberataques, a lo largo de la Primera Parte del presente estudio.

En relación con el tema que aquí se aborda, en una visión preliminar del texto del Proyecto, el Estado no será responsable de la violación de una norma de DIH, si ésta se comete en legítima defensa. Esta previsión obliga a despejar incógnitas tales como si resulta conforme al DIH la respuesta, en legítima defensa, frente a una ciberoperación o si frente a un ataque armado, en el que se emplea la fuerza cinética, cabe responder en legítima defensa por medios informáticos. Asimismo, el estudio de los requisitos y límites de la legítima

721 Así se expresa también GUTIERREZ ESPADA al entender que únicamente frente a un ataque armado será posible la legítima defensa. GUTIÉRREZ ESPADA, C., *La responsabilidad internacional del Estado por uso de la fuerza armada (la conformación del hecho ilícito internacional)*. Cursos de Derecho Internacional de Vitoria-Gasteiz, 1989. Servicio editorial de la Universidad del País Vasco, Bilbao, 1990; pp. 189-310, en particular, p. 279.

722 CASANOVAS Y LA ROSA expone que, "*según el Derecho Internacional Consuetudinario la legítima defensa del Estado agredido debe ser una respuesta inmediata, necesaria y proporcional al ataqu*e". CASANOVAS Y LA ROSA, O. *El principio de prohibición del uso de la fuerza*, op. cit.; p. 1073.

723 Asi lo expresa HOISINGTON, al citar, en el mismo sentido a JENSEN: "*whether cyberwarfare constitutes a use of force giving rise to the right of self-defense therefore represents an important question in international law*". HOISINGTON, M. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. Boston College International and Comparative Law Review, vol. 32, 2009; pp. 439-454, en particular, p. 440.

defensa, cobra aquí una especial relevancia, siempre teniendo presente que un análisis exhaustivo de los mismos excede el propósito del presente subepígrafe y que, por lo tanto, se abordarán los aspectos imprescindibles para concluir si, la reacción en legítima defensa puede o no eximir de responsabilidad internacional al Estado.

En una primera aproximación, cabe afirmar que la respuesta en legítima defensa no puede ser ilimitada, ni tratada de forma autónoma, a la vista de lo dispuesto en el Proyecto, sino que ha de estar sujeta a las restricciones que la Carta de Naciones Unidas impone. Éstas han sido, tradicionalmente, reconocidas por la Jurisprudencia Internacional, que ha exigido la observancia de los principios de DIH[724] . En este sentido, nuevamente, ha de traerse a colación la Opinión Consultiva relativa al uso de las armas nucleares, emitida por la CIJ, ya que, en palabras de DOSWALD-BECK, "*en los párrafos 41 y 42 de su Opinión, se declara de acuerdo con la opinión según la cual se aplican las restricciones de ambos ámbitos jurídicos*[725]"; es decir, la Corte aclara que la legítima defensa ha de observar los principios del DIH, cuando establece que,

> "The submission of the exercise of the right of self-defence to the conditions of necessity and proportionality is a rule of customary international law. As the Court stated in the case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) : there is a "specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law" (I. C. J. Reports 1986, p. 94, para. 176). This dual condition applies equally to Article 51 of the Charter, whatever the means of force employed".

Por otra parte, cabría plantearse si estas limitaciones se aplican a los

724 Así lo requiere la Corte en el párrafo 42 de la citada Opinión Consultiva, al afirmar: "*The proportionality principle may thus not in itself exclude the use of nuclear weapons in self-defence in al1 circumstances. But at the same time, a use of force that is proportionate under the law of self-defence, must, in order to be lawful, also meet the requirements of the law applicable in armed conflict which comprise in particular the principles and rules of humanitarian law*". Legality of the Threat or Use of Nuclear Weapons uclear weapons, doc. ci.; par. 42.

725 DOSWALD-BECK, L., *El derecho internacional humanitario y la Opinión consultiva de la Corte Internacional de Justicia sobre la licitud de la amenaza o del empleo de armas nucleares*, doc. cit.

ciberataques o si su naturaleza impide una completa traslación de estos requisitos. Pues bien, en este sentido, parece que de la Jurisprudencia internacional se deduce una respuesta afirmativa[726].

Así, una vez que el Estado sufra un ciberataque armado estará legitimado, en virtud de lo dispuesto en el artículo 51 de la Carta, a hacer frente al mismo, pues este derecho resulta inherente a la soberanía de los Estados y se configura como un reflejo positivo del Derecho Consuetudinario[727]. La legítima defensa entrará en juego, por lo tanto, en todos aquéllos supuestos en los que el Estado sufra un ataque armado o agresión ilegítima y, por lo tanto, con independencia de la naturaleza de las armas empleadas en el ataque y de si éstas constituyen fuerza armada convencional o virtual, tendrá que reconocerse al Estado la posibilidad de defenderse de dicho ataque armado[728]. Tampoco los autores del Manual de Tallin han dudado en reconocer el inherente derecho de los Estados al ejercicio de la legítima defensa, en cuestiones de ciberdefensa[729].

Pues bien, reconocido tal derecho, es preciso analizar las circunstancias que han de estar presentes para que el mismo resulte conforme a Derecho. En este sentido, hay que comenzar precisando que los límites impuestos al ejercicio del derecho de legítima defensa han sufrido una evolución a lo largo del tiempo, cuyo estudio se realizará de forma breve. En lo que aquí resulta de interés, se hará referencia a la decisión que podría ser considerada como un punto de inflexión en la concepción del ejercicio de la legítima defensa. La Resolución 1368 del Consejo de Seguridad de Naciones Unidas de 2001, dictada como consecuencia de los atentados acaecidos el 11 de septiembre del mismo año, en territorio de los Estados Unidos, bien puede ser considerada así. A esta

726 En concreto, la CJI, en la Opinión Consultiva aludida, expresamente afirma que "*These requirements of Article 51 apply whatever the means of force used in self-defence*". Legality of the Threat or Use of Nuclear Weapons, doc. cit.; pár. 44.

727 Los autores del Manual de Tallin, así lo expresan, al aludir al artículo 51 de la Carta de Naciones Unidas , diciendo " *This article recognizes and reflects the customary right of self-defence*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p. 54.

728 Esta constituye una de las conclusiones del grupo de expertos, autores del Manual de Tallin, que afirman que, además, esta aseveración es práctica común entre los Estados y que se justifica, "*despite their non-kinetic nature, because the ensuing consequences can include serious suffering or death. Identical reasoning would apply to cyber operations*". SCHMITT, M.N. (General Editor). Tallin Manual op. cit.; p. 55

729 *Ibidem*, pp. 53-64.

conclusión ha de llegarse tras el examen del escueto texto de la misma que, una vez que califica los hechos como atentado terrorista, reconoce el derecho al ejercicio de la legítima defensa frente a los mismos.[730] En el presente supuesto, nada hubiera impedido el reconocimiento del derecho a la legítima defensa si el hecho ilícito hubiera sido atribuido a un Estado, en los términos que ya fueron expuestos al abordar la cuestión de la atribución. Sin embargo, *a priori*, no parece coherente con la regulación del uso de la fuerza, que realiza la Carta de Naciones Unidas, la calificación del hecho como atentado terrorista y, posteriormente y sin solución de continuidad, reconocer un derecho a la defensa que, necesariamente, se desarrolló en territorio de un Estado, al que no se le había atribuido formalmente dicho ilícito. Por otra parte, tampoco parece que la agresión pudiera responder a la definición de "agresión indirecta", que pudiera justificar tal respuesta, pues en la construcción jurídica de la misma, se presenta como esencial que la misma se cometa por "*un movimiento armado interno, nacido o establecido en otro [Estado], en su lucha contra el Gobierno de ese Estado*", siempre y cuando "*pueda demostrarse el control absoluto de dichos grupos por parte del Estado en cuestión*[731]".

En consecuencia, las cuestiones que hasta ahora han sido tratadas, en relación al concepto de ataque armado, de atribución del mismo al Estado y de aplicación del DIH a los agentes no estatales, vuelven a cobrar de nuevo relevancia en el estudio de la reacción del Estado en legítima defensa. Así se desprende del contenido de esta Resolución pues, como recoge CASANOVAS Y LA ROSA, determinados autores llegaron a cuestionar, en primer lugar, que los ataques ocurridos en 2001 en los Estados Unidos, tuvieran la consideración jurídica de ataque armado. En consecuencia, el ejercicio de la legítima defensa, en

730 La Resolución afirma la existencia de un ataque terrorista: "*Decidido a combatir por todos los medios las amenazas a la paz y la seguridad internacionales creadas por actos de terrorismo*". Posteriormente se manifiesta: "Reconociendo el derecho inmanente de legítima defensa individual o colectiva de conformidad con la Carta de las Naciones Unidas". Resolución 1368 (2001), aprobada por el Consejo de Seguridad, en su 4370ª sesión, de 12 de septiembre de 2001. Doc. S/RES/1368 (2001).

731 Dicha definición puede contemplarse en GUTIÉRREZ ESPADA, C., *La responsabilidad internacional del Estado por uso de la fuerza armada (la conformación del hecho ilícito internacional),* op. cit.; p. 255.

respuesta al mismo, quedaba igualmente cuestionado, "*dado que no hubo intervención de las fuerzas armadas de ningún Estado*[732]". A mayor abundamiento, la respuesta en legítima defensa que se produjo cuestiona, asimismo, si la actuación reunía los requisitos de inmediatez, provisionalidad y subsidiariedad.

Parece evidente que esta nueva línea conceptual y argumental emprendida por Naciones Unidas, entraña ciertos riesgos en relación a la seguridad jurídica, deseable en la regulación de las relaciones jurídicas aplicables a la Comunidad Internacional. Como se ha puesto de relieve en otra parte del presente trabajo, la aplicación del DIH a sujetos terroristas o la atribución de la categoría de terroristas a determinados combatientes no supone una cuestión sencilla, ni carente de trascendentes consecuencias jurídicas. Por este motivo, resulta poco deseable la confusión conceptual que la Resolución parece reflejar. Por otra parte, esta disipación de los límites, hasta ahora conocidos, podría generar una mayor confusión, a la hora de introducir elementos de agresión novedosos, como el que aquí se estudia.

En este sentido, los ejemplos que aquí se han expuesto ponen de manifiesto que pocas veces la presencia de un ciberataque armado estará completamente clara. Antes bien, la experiencia demuestra que, en numerosas ocasiones, se han producido pequeños ataques en forma de goteo, que han sido lanzados contra un Estado, sin que ninguno de ellos llegara a presentar la relevancia y entidad suficiente, para calificarlo jurídicamente como un ataque armado que justificara una reacción en legítima defensa. También conviene reiterar que estos supuestos bien podrían constituir un hecho ilícito. Sin embargo, la imposibilidad de calificarlos como ataque armado, impediría la exención de responsabilidad internacional con base en esta causa justificativa [733] .

732 Así se expresa CASANOVAS Y LA ROSA, citando a GUTIÉRREZ ESPADA. CASANOVAS Y LA ROSA, O. *El principio de prohibición del uso de la fuerza.* Instituciones de Derecho Internacional Público. DIEZ de VELASCO, Tecnos. Madrid 2013; pp. 1067-1096, en particular, p. 1077.

733 Así se expresa igualmente GROSWALD, al afirmar que "*Intermittent, small-scale cyberattacks could take advantage of the gap between Articles 2(4) and 51. If cyberattacks are small enough, they might be considered a use of force but not an armed attack significant enough to trigger the victim's right of self-defense under Article 51. In contrast, a series of small-scale attacks might constitute an armed attack under Article 51, but local law enforcement might treat each attack as a separate incident rather than parts of a larger attack. (…). Attributing the origin of a cyberattack and effects of an attack to a state are vital in complying with the requirements of self-defense under international law. The pervasiveness of non state*

Precisamente por ello no parece que la aceptación de la legítima defensa, en relación con ataques terroristas, vaya a contribuir a la clarificación de nuevas situaciones.

Esta extensión del concepto de legítima defensa, que se permite contra actos que no son ataques armados, tal como quedan recogidos en la Carta de Naciones Unidas, podría originar, además, un uso desmedido de la reacción en legítima defensa que, lejos de reprimir y evitar la violencia, la multiplique y difunda. Como recuerda EYMAR ALONSO, "*para que un Estado pueda invocar con fundamento la legítima defensa para utilizar la fuerza, debe cumplir con los dos requisitos básicos que se derivan de lo dispuesto en el citado artículo 51, esto es: a) ser objeto de un ataque armado; b) ejercer la fuerza de forma provisional hasta que el Consejo de Seguridad adopte las correspondientes medidas*[734]". Y, como expone REGUEIRO DUBRA, no puede olvidarse que, además de los requisitos contemplados en la Carta de Naciones Unidas, la Jurisprudencia Internacional ha apuntado la existencia de otros de naturaleza consuetudinaria[735].

Así, la presencia de un ciberataque armado se producirá, únicamente, cuando puedan comprobarse los criterios expuestos en el Capítulo Primero del presente trabajo, sin que convenga abandonar el criterio restrictivo allí defendido, y el resto de ataques informáticos caerá dentro del ámbito delictivo, de forma que será perseguible, en tanto que los mismos supongan una contravención del Derecho interno.

Asimismo, en el caso de que se trate de ataque terroristas difundidos por la red, en el modo que también ha sido examinado, no podrá otorgarse, sin más, la calificación de ataque armado y, por lo tanto, será ineficaz la invocación de la legítima defensa, siempre teniendo en cuenta los matices ya expuestos en el

---

actors on the Internet and their ability to disguise their tracks requires that the concept of attribution not only remain in place, but be reinforced. Thus, in order to prevent innocent deaths and collateral damage, "getting it right" is of extreme importance." GROSSWALD, L., Cyberattack Attribution Matters Under Article 51 of the U.N. Charter. Brooklyn Journal of International Law vol. 36, issue 3. 2011; pp. 1151-1181, en particular, pp.1176 y 1177.

734 EYMAR ALONSO, C., *Estados Unidos y la cuestión de la legítima defensa preventiva. Grupo de Estudios Estratégicos, op. cit.*

735 REGUEIRO DUBRA, R. La Legítima Defensa en Derecho Internacional. Instituto Universitario General Gutiérrez Mellado. UNED 2012; p. 93. Disponible en el sitio web: http://iugm.es/publicaciones/colecciones/libros-investigacion. Fecha de consulta enero de 2015.

estudio de las cuestiones relativas a la atribución del hecho ilícito. En cualquier caso, la adopción de un criterio restrictivo se revela necesario para garantizar una adecuada aplicación de los criterios exigidos para la legitimidad de la defensa, individual o colectiva. Como ejemplo de ello, baste citar nuevamente los ataques dirigidos a Estonia. En dicha situación, la adopción de medidas en legítima defensa hubiera sido tan novedosa, como en el caso de los ataques terroristas a los Estados Unidos, pues nunca antes un Estado se había encontrado ante una situación de disfunción cibernética similar, como consecuencia de hechos externos. El análisis de la situación y de su respuesta eran, pues, *a priori*, susceptibles de interpretación. Sin embargo, parece claro que esta respuesta no podía realizarse de forma clara, al no estar despejadas todas las incógnitas en relación con la atribución de la conducta, de forma que, con toda probabilidad, la respuesta hubiera sido errónea.

No obstante, ello no puede llevar a la conclusión de que ante un hecho ilícito que constituya un ataque armado cometido a través de un método de combate cibernético, la legítima defensa tenga que ser descartada de antemano. Antes bien, tal y como afirma la doctrina internacionalista, puede aseverarse que "*international law governs activities in cyberspace and that states maintain sovereignty rights as well as the right to defend against threats in cyberspace*[736]". En consecuencia, el comportamiento que, en el ámbito internacional, se exige a los Estados que sufren ataques convencionales o que se defienden por medios convencionales, ha de ser exigido en el uso de internet. Se trata, además, de otra oportunidad de favorecer e incentivar el protagonismo de los Estados en el ámbito internacional, de forma tal que impida el crecimiento de la intervención de actores no estatales, como ya se ha producido en la práctica[737], que aboga otro sector de la doctrina internacionalista[738].

736 LOTRIONTE, C., *State sovereignty and self-defense in cyberspace: a normative framework for balancing legal rights*, op.cit.; p. 831.

737 "*(...) the United States has continued the use of the armed drones against individual terrorists in other states such as Yemen, Syria, and Pakistan. This indicates that the U.S. will continue to use force in self-defense against non-state actors even if they may reside in states against which the United States is not in armed conflict*". *Ibidem*, p. 877.

738 En este sentido, KESAN y HAYES entienden que, "*Since the language seems to permit it and the reality of cyber warfare may even require it, it's possible that considerations relating to articles of the U.N.*

Cuando estas conclusiones se trasladan al específico ámbito de la causa de justificación de la conducta, hay que partir de los mismos supuestos y, por lo tanto, podrá afirmarse que la violación de la obligación internacional quedará justificada cuando el hecho ilícito se cometa en legítima defensa y ésta sólo concurrirá cuando se acrediten los requisitos de legalidad que van a exponerse.

La acreditación del primer requisito, *i.e.*, la existencia de un ataque armado, ha sido objeto de pronunciamiento por la Jurisprudencia internacional que, en la Sentencia dictada con ocasión de las Actividades Militares y Paramilitares en Nicaragua[739], afirmó que

> "In the case of individual self-defence, the exercise of this right is subject to the State concerned having been the victim of an armed attack. (...). There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein". This description, contained in Article 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces. But the Court does not believe that the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the interna1 or external affairs of other States".

Sin embargo, la traslación de conceptos al ámbito cibernético no siempre resulta tan sencilla, por lo que han de abandonarse tradicionales criterios

---

Charter should be interpreted as potentially applying to private actors in the context of cyberspace where national boundaries are at best amorphous". KESAN, J.P. and HAYES, C. M., Self Defense in Cyberspace: Law and Policy. Illinois Public Law and Legal Theory Research Papers Series No. 11-16; pp. 1- 36, en particular, 11-12.

739 Military and Paramilitary Activities in and against Nicaragua, doc. cit.; par. 195.

defendidos por la doctrina, como el de la territorialidad, pues la virtualidad del elemento que aquí se analiza impide circunscribir el hecho ilícito y la respuesta al mismo a un territorio determinado. Bien es cierto que dicho requisito puede ser salvado a través de la atribución de la conducta, de forma tal que la autoría de un Estado no requiera del elemento territorial[740], aunque también este concepto ha sido objeto de redefinición, que ha originado la adopción del término "ciberterreno"[741].

Por último, aspectos tales como la proporcionalidad de la respuesta, la inminencia del ataque y la inmediatez de la defensa, requieren un análisis en relación al ataque armado y a la respuesta que al mismo se ofrezca, ya se articulen éstos, a través de medios convencionales o cibernéticos. Por este motivo, entre otros, el estudio de la proporcionalidad de la defensa y el momento de ejercerla cobran un nuevo significado.

La necesidad ha sido definida como la fuerza necesaria para repeler el ataque armado que se está produciendo[742]. Es decir, que la agresión o ataque no pueda ser repelido de otro modo, que el Estado agredido se encuentre ante una falta de alternativa y, por último, la necesidad ha de ser razonable, "*atendidas las*

740 En este sentido, REGUEIRO DUBRA sostiene que "*un ataque armado, sea el hecho de agentes del Estado (sus órganos) o de particulares (sin relación prima facie con el Estado), debe ser atribuible a un Estado determinado, porque de no ser así, ¿en qué territorio se va a ejercer la legítima defensa?*". REGUEIRO DUBRA, R. *La Legítima Defensa en Derecho Internacional,* op. cit; p. 93.

741 Así, por ejemplo, DEWEESE, en relación a estas cuestiones, afirma "*Part of any cyber operation involves first probing, then gaining access to targeted networks. This has been referred to as the process of identifying key cyber terrain (…). cyber maneuver which was defined as "the application of force to capture, disrupt, deny, degrade, destroy or manipulate computing and information resources in order to achieve a position of advantage in respect to competitors." While in the kinetic world, maneuver would involve the actual movement of military forces, in the cyber context, it involves using code to achieve its purpose (…). The probable use of cyber operations by Israel to disable Syrian air defense systems prior to a 2007 Israeli air attack on a suspected nuclear power plant in Syria is offered as an example of this type of maneuver. In that example, Israeli aircraft were able to fly into Syrian airspace without detection and achieve their objective and destroy the plant*". DEWEESE, G.S., *Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence*. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace M. Maybaum, A.-M.Osula, L.Lindström (Eds.). 2015 NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn 2015; 81 a 92, en particular, pp. 88 y 89.

742 Así se define por parte de los autores del Manual de Tallin "*It merely requires that non-forceful measures be insufficient to address the situation. Of course, the forceful actions may be combined with non-forceful measures such as diplomacy, economic sanctions, or law enforcement*". SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p. 61.

circunstancias[743]".

En cualquier caso, la agresión que se repele ha de ser coetánea a la acción defensiva. La tendencia, dentro de la doctrina internacionalista[744], que aboga por la admisión de la llamada legítima defensa anticipada, ha de ser firmemente rechazada por resultar contraria a las exigencias de la legalidad internacional, que exige que la legítima defensa se produzca en el momento en que "*an armed attack occurs*".

Sin embargo, la tendencia apuntada en la doctrina resulta ciertamente relevante y, como pone de manifiesto CRONDOM, "*Other legal scholars argue that Article 51 incorporates customary international law as articulated by the Caroline standard, allowing anticipatory selfdefense*"[745]. Nuevamente, se pone de relieve la dificultad de atribución de la conducta y la disparidad de consecuencias, en función de si la misma ha sido realizada por el Estado o por un agente no estatal. Determinados autores sostienen la tesis de que el Estado no ha de verse constreñido a la hora de ejercer su legítima defensa[746]. No obstante, se trata de una interpretación y de una tendencia, en la práctica de los Estados, que debería ser rechazada por cuanto la asunción de tesis extensivas constituiría una interpretación *contra legem* de la legalidad internacional[747].

En el estudio de las cuestiones relativas a la exención de la responsabilidad

---

743 *Ibidem*, p. 60.

744 Dentro de este sector doctrinal también puede incluirse al sector mayoritario del grupo de Expertos del Manual de Tallin, que refleja: "*The majority of the International Group of Experts took the position that even though Article 51 does not expressly provide for defensive action in anticipation of an armed attack, a State need not wait idly as the enemy prepares to attack. Instead, a State may defend itself once the armed attack is 'imminent'. Such action is labelled 'anticipatoryself-defence'*". *Ibidem*, p.60

745 CONDRON, S. M. Getting it right: protecting american critical infrastructure in cyberspace. Harvard Journal of Law & Technology, vol. 20, Number 2 Spring 2007; pp. 404-422, en particular, pp.412-413.

746 Así lo afirma HOISINGTON, al entender que "*Restraining a state's ability to respond will encourage rogue nations, terrorist organizations, and individuals to commit increasingly severe cyberattacks*". HOISINGTON, M. ,*Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, op. cit.; p. 452.

747 "*Despite the wording of Article 51, many States interpret the language as more permissive and inclusive of anticipatory actions as a customary international law norm. Under this view, a State is "not required to absorb the first hit before it can resort to the use of force in selfdefense to repel an imminent attack. Indeed, even those who advocate a strict interpretation of Article 51 recognize that history is replete with instances where States have resorted to anticipatory actions in self-defense*". DEWEESE, G.S., Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence, op. cit.; p. 83.

internacional, la definición de la legítima defensa anticipada como aquella acción que se presenta al Estado como la única alternativa, sin que haya ocasión de deliberar[748], bien podría ser confundida con otras causas ya citadas como el estado de necesidad o el peligro extremo. En estos casos, ya se ha examinado cómo el comportamiento antijurídico del Estado queda amparado por unas circunstancias que impiden que el mismo actúe de otro modo, siempre y cuando la violación de la obligación internacional no constituya una infracción de las normas de *ius cogens*.

No obstante, en este punto, los autores que defienden la legítima defensa anticipada, abogan erróneamente por invocar la legítima defensa, en caso de ausencia de alternativa o de tiempo para reaccionar cuando, en realidad, estos supuestos entrarían en la definición de estado de necesidad que ya se ha visto. La legítima defensa exige la existencia de una agresión de la que el Estado se defienda y esa agresión sólo puede ser coetánea a la defensa, pues, en caso contrario, la reacción del Estado habría de calificarse como represalia o bien, en el caso de ser anterior, como ataque, pero en modo alguno como defensa.

La legítima defensa, ejercida con carácter previo al ataque, puede conllevar, además, la asunción de un riesgo innecesario, teniendo en cuenta las dificultades que se han constatado en la atribución del hecho ilícito, incluso cuando éste ya se ha consumado. Como se ha expuesto en el análisis del resto de causas de justificación, la atribución del ilícito vuelve a ser clave a la hora de invocar la justificación de la conducta del estado infractor. En modo alguno podrá invocarse una defensa legítima si el agresor no ha sido identificado. De entre los ejemplos que se han ido explicando en los capítulos precedentes, resulta de interés ahora volver al ataque producido por el virus Stuxnet, en la central

748 KESAN y HAYES, tratan la legítima defensa anticipada en los siguientes términos: "*International law also includes the concept of anticipatory self-defense, which is permitted when the need for self-defense is instant and overwhelming, there is no other way to respond, and there is no time for deliberation. The immediacy requirement of anticipatory self-defense is relative to the strength of the state, and requires that the aggressor has committed to an armed attack and that the defender's ability to defend itself would be hindered if it waited to respond. If there is evidence of an ongoing campaign against a state, anticipatory self-defense may be authorized because future armed attacks are considered imminent*". KESAN. J. P. y HAYES, C. M., Self Defense in Cyberspace: Law and Policy, op.cit.; p. 16.

nuclear de Irán[749]. En su momento ya hubo ocasión de analizar el modo en que el virus actuó en el sistema informático de la instalación nuclear. En este punto, el ejemplo resulta útil para ilustrar la inconveniencia de defender las tesis anticipatorias expuestas. Además, como pone de relieve BERMEJO GARCIA, "*hay que reconocer que entre lo inminente y lo latente puede haber diferencias importantes en muchos casos, pero en otros esas diferencias se mitigan considerablemente*".[750]

Si, desde un punto de vista estrictamente teórico, estudiamos el lanzamiento del virus Stuxnet como respuesta a la amenaza nuclear, en ese momento sostenida por el Estado de Irán, puede comprobarse cómo la necesidad de que la agresión y la reacción sean coetáneas no es superficial. En efecto, aun cuando por algunos autores se ha sostenido que el comportamiento de Irán constituía una amenaza inminente[751], sin embargo, la respuesta se produjo de forma muy anticipada a la verdadera amenaza, pues no se tuvo constancia de ninguna manifestación concluyente al respecto[752]. De este modo, tal y como en otro apartado ha sido expuesto, se produjeron unos daños adicionales al objetivo a abatir que, en todo caso, debieran haberse evitado. La inexistencia de una

749 Al respecto, REGUEIRO DUBRA expone, "*Desde que, en 2002, se descubrió que Irán desarrollaba clandestinamente actividades nucleares, la preocupación se centró en la posibilidad de que el programa iraní no fuese realizado con fines pacíficos, sobre todo teniendo en cuenta que el Presidente de Irán, Mahmud Ahmadineyad, no dudó en declarar en repetidas ocasiones que Israel debía ser borrado del mapa y que el holocausto no era nada más que un "mito inventado por Occidente*" y que el "Consejo de Seguridad ha adoptado una nueva resolución en la que reiteró que Irán había incumplido sus resoluciones anteriores y, por ello, amplió el círculo de personas y entidades objeto de las sanciones adoptadas". La Resolución a que se hace referencia es S/RES/1929 (2010), de 9 de junio. REGUEIRO DUBRA, R. La Legítima Defensa en Derecho Internacional, op. cit.; pp. 366 y 369.

750 BERMEJO GARCIA, R. ¿*Puede la legitima defensa ponerse en un sitio? Algunos comentarios y reflexiones*. Estudios de Derecho Internacional y de Derecho europeo en homenaje al Profesor Manuel Pérez González. Tomo I. Aznar Gómez, M., (Coordinador). Tirant lo Blanch. Valencia, 2012; pp. 209-236, en particular, p. 236.

751 Como recoge KILOVATY, "*On the contrary, and arguably, the cyber attack on Natanz could be justified by anticipatory self-defense against an imminent threat*". KILOVATY, I., *Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare*. National Security Law Brief 5, no. 1.2014; pp. 91-124, en particular, p.92.

752 En este ámbito se comparte la opinión de REGUEIRO DUBRA cuando afirma que "*no existe amenaza a nuestro parecer, aunque de existir no sería suficiente para dar paso al ejercicio del derecho de legítima defensa al no ser asimilable a un ataque armado en el sentido del artículo 51 de la Carta. Tampoco existe amenaza inminente de ataque que permitiría a los Estados que pudieron ser objetivo invocar el derecho a defenderse*". REGUEIRO DUBRA, R. La Legítima Defensa en Derecho Internacional, op. cit; p. 373.

agresión previa impide considerar este ciberataque como una respuesta en legítima defensa, pues, de lo contrario, se estaría legitimando el uso de la fuerza ante una agresión supuesta. Toda vez que ya ha sido objeto de atención en otra parte del presente trabajo, no procede ahora ahondar en la calificación jurídica de este ciberataque, más allá de reiterar la imposibilidad de tenerlo por una respuesta en legítima defensa. Antes bien, se ha planteado por parte de cierto sector doctrinal, incluso la posibilidad de que el Estado de Irán hubiera estado legitimado para responder ante dicho ataque[753]. En efecto, el lanzamiento de este virus lleva a cuestionar si nos encontrábamos ante un ataque armado, aunque haya sido calificado como un acto de espionaje o de mero sabotaje[754]

La legítima defensa, pues, desplegará sus efectos siempre y cuando cumpla con los requisitos que tradicionalmente han sido exigidos y que, como señala EYMAR ALONSO, se circunscriben a "(...) *que: i) la agresión (ataque armado) esté en curso; y, ii) ha de atajarse cuando las instituciones comunes toman las medidas pertinentes (subsidiariedad), es decir: "hasta tanto que el CS haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales*[755]".

Sin embargo, en relación al primer requisito, quienes abogan por la legitimidad de la defensa anticipada entienden que es suficiente que un ataque armado esté *a punto* de ser lanzado[756]. No es esta postura tampoco compartida por los autores del Manual de Tallin, que rechazan el criterio temporal en el ámbito de la respuesta a ciberataques o por medio de éstos[757]. En cualquier caso,

753 Así lo pone de manifiesto LOTRIONTE al entender que, "in assessing whether Iran may have had a legal right to use force in self-defense against the state or states responsible for targeting its uranium facility with the Stuxnet worm, assuming a state was responsible, Iran would have no right of selfdefense once the cyber attack stopped and the threat of attacks no longer existed. If the victim state did use force after the attacks were over and the threat was no longer, it would likely be an act of reprisal and illegal under international law. If an attack is imminent, however, the circumstances may be that there is no time to pursue other measures and the victim state acts necessarily, invoking its right of self-defense". LOTRIONTE, C. *State sovereignty and self-defense in cyberspace*, op. cit.; p.891.

754 GILL, T. D and DUCHEINE, P. A. L., Anticipatory Self-Defense in the Cyber Context. International Law Studies. U.S. Naval War College. 2013. Vol., 89; pp. 438-471, en particular, p.463.

755 EYMAR ALONSO, C., Estados Unidos y la cuestión de la legítima defensa preventive, op. cit.

756 SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p. 61.

757 Así lo explican al afirmar que, "*The critical question is not the temporal proximity of the anticipatory defensive action to the prospective armed attack, but whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts*". En este caso, es más que imprescindible tener presente el momento en que se

la valoración unilateral por parte del Estado de cuestiones tales como, si el ataque va a producirse o no y su inminencia, empobrece considerablemente la limitación del uso de la fuerza por parte de los Estados a la que aspira la organización de Naciones Unidas y, a su vez, supone una amenaza clara a la legalidad internacional.

Si con carácter general ha de rechazarse la asunción de esta postura, con mayor razón en el caso del lanzamiento de ciberataques, ya constituyan éstos la inicial agresión, ya sean empelados como modo de defensa. En el supuesto concreto que aquí se estudia, es decir, la defensa a través de ciberataques que violen una norma de DIH, parece razonable asumir la tesis de que se ejerza, únicamente, frente a agresiones constatadas, por más que dicha constatación, como reiteradamente se ha puesto en evidencia, conlleve una mayor dificultad que si se produjera por métodos de combate tradicionales[758].

En estos casos, de nuevo la doctrina internacionalista pretende hacer valer posturas que pudieran entenderse asumibles desde un punto de vista práctico, pero cuestionables a la luz de la legalidad internacional, desde el momento en que se aboga por un "*right of self-defence in the face of armed attacks by non-State actors, such as terrorist or rebel groups*[759]". Así, los autores del repetido Manual de Tallin, entienden que dicha posibilidad ha de extenderse a los casos de ciberataques. Sin embargo, sin ánimo de ahondar en tesis que ya han sido expuestas, los argumentos antes enunciados, junto con las dificultades de atribución señaladas en el epígrafe correspondiente y de aplicación del DIH a terroristas y grupos rebeldes, desaconsejan ahondar en la práctica sugerida por estos autores. Otros autores, considerando la necesidad de residenciar la

---

produce la respuesta en defensa, pues, "*The requirement of immediacy (as distinct from the requirement of imminence discussed above) distinguishes an act of self-defence from mere retaliation*". SCHMITT, M.N. (General Editor). Tallin Manual; op. cit.; p. 62.

758 HOISINGTON al respecto, propone que "*While it is difficult to discover the identity of the attacker, identifying his or her intent in time to take preventive action represents an equally problematic and potentially more important task. (…) Walter Gary Sharp has proposed that all states should adopt a rule of engagement that allows them to use force in anticipatory self-defense against any identified state that demonstrates hostile intent by penetrating a computer system which is critical to their respective vital national interests*". HOISINGTON, M., *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, op. cit.; p. 451.

759 SCHMITT, M.N. (General Editor). Tallin Manual, op. cit.; p. 60.

responsabilidad internacional únicamente en los Estados, llevan este argumento al límite de considerar que, en el ámbito de la legítima defensa, "*because the evidentiary standards required for attribution present insurmountable barriers for injured states, strict liability should be imposed on states that either did not or could not prevent a terrorist attack from emanating within its borders*[760]".

La inminencia del ataque frente al que se responde, no obstante, también conllevará riesgos en el discernimiento de la respuesta adecuada. Sin entrar ahora en cuestiones de proporcionalidad que se verán más adelante, la distinción entre la agresión que justifica la legítima defensa o, por otra parte, la invocación del peligro extremo, conllevará ciertas dificultades.

Como se ha visto, la violación de una norma de DIH durante el combate impide la exigencia de responsabilidad internacional cuando el Estado, a través del lanzamiento del ciberataque no tenga "*razonablemente otro modo, en una situación de peligro extremo, de salvar su vida o la vida de otras personas confiadas a su cuidado*". Se trata por ende, de una situación de tal magnitud, que el bien jurídico en juego es únicamente la vida, mientras que la respuesta en legítima defensa podrá darse frente a cualquier otro peligro, siempre que dicha respuesta se realice en proporción a la agresión causada. Por último, conviene recordar que los ataques informáticos que hasta ahora han tenido una mayor relevancia para la doctrina internacionalista, responde más a la configuración del hecho ilícito continuado, tal como también quedó analizado en otra parte del presente que a la realización de un único acto. En consecuencia, remitiéndonos a lo allí expuesto, hay que precisar aquí que "*La exigencia del carácter inmediato de la acción ejecutada en legítima defensa deberá apreciarse con arreglo al conjunto de esos actos*[761]".

760 Así lo afirma, GROSSWALD, citando a PROULX , V.-J., GROSSWALD, L., *Cyberattack Attribution Matters Under Article 51 of the U.N. Charter*, op. cit.; p. 1165.

761 Fifth report on State responsibility by Mr. Roberto Ago, Special Rapporteur - the internationally wrongful act of the State, source of international responsibility (continued), doc. cit; párr. 122.

2.2. La proporcionalidad en la respuesta por medios cibernéticos y convencionales.

La proporcionalidad en la respuesta, como ha quedado apuntado, ha sido señalada por la Jurisprudencia Internacional, como un requisito de legalidad, de naturaleza consuetudinaria. En el pronunciamiento relativo a las actividades militares y paramilitares en y contra Nicaragua, la CIJ tuvo ocasión de establecer que

> "there is a "specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law. This dual condition applies equally to Article 51 of the Charter, whatever the means of force employed.[762]".

De este modo, la necesidad de la defensa se comprobará en tanto que exista necesidad de hacer uso de la fuerza y, en el caso de la proporcionalidad, habrá que comprobar la medida que haya de tener dicha fuerza, teniendo siempre presente la estrecha relación entre ambos conceptos[763].

El uso de métodos de combate informáticos, en caso alguno impedirá la exigencia de este requisito, aunque no se pueda afirmar que la proporcionalidad implique que, para defenderse, haya que hacer uso de medios idénticos a los empleados en el ataque que se repele, pues podremos encontrarnos ante situaciones en las que "*cyber use of force may be resorted to in response to a kinetic armed attack, and vice versa*[764]". En consecuencia, cuando un Estado en conflicto reciba un ataque armado informático estará legitimado para responder a través de métodos convencionales y viceversa, siempre en función del contexto en que se desarrolle el mismo[765].

762 Military and Paramilitary Activities in and against Nicaragua, doc.cit; par. 176.
763 Al respecto, KRETZMER entiende que "*Means can only be proportionate when they are necessary to achieve the legitimate ends*". KRETZMER, D., *The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum*. European Journal of International Law, vol. 24, no. 1, 2013; pp. 235–282, en particular, p. 239.
764 SCHMITT, M.N. (General Editor). Tallin Manual, op.cit; p. 60.
765 Esta posibilidad también es contemplada por los autores del Manual de Tallin que, en la Norma 14, entre otras afirmaciones se sostiene que "*there is no requirement that the defensive force be*

Este requisito de la proporcionalidad ha sido ampliamente tratado por la doctrina internacionalista y, en este caso, va a ser uno de los más difíciles de definir a la hora de introducir el elemento cibernético[766]. Sin embargo, como repetidamente se ha puesto de manifiesto, las dificultades que entraña la utilización del método de combate cibernético, no pueden conllevar la flexibilización en la exigencia del cumplimiento de la legalidad internacional. No puede obviarse que los Estados encontrarán serias dificultades a la hora de atribuir un ciberataque armado a otro Estado, al decidir sobre la necesidad del uso de la fuerza para detenerlo y, posteriormente, al calibrar la medida de esa fuerza, pero ello no puede desembocar en una exención del control de legalidad en su actuación[767].

En este punto, es necesario recordar la Opinión Consultiva en relación al uso de las armas nucleares, pues la CIJ estableció, nítidamente, que

> "The proportionality principle may thus not in itself exclude the use of nuclear weapons in self-defence in all circumstances. But at the same time, a use of force that is proportionate under the law of self-defence, must, in order to be lawful, also meet the requirements of the law applicable in armed conflict which comprise in particular the principles and rules of humanitarian law"[768].

---

of the same nature as that constituting the armed attack. Therefore, a cyber use of force may be resorted to in response to a kinetic armed attack, and vice versa. The proportionality requirement should not be overstated. It may be that the originator of the cyber armed attack is relatively invulnerable to cyber operations. This would not preclude kinetic operations in an effort to compel the attacker to desist, although they must be scaled to that purpose". SCHMITT, M.N. (General Editor). Tallin Manual, op.cit.; p. 60.

766 También en este sentido se expresa LOTRIONTE al afirmar que "*In cyber operations, the deployment of computer code in self-defense targeted to stop an attack may pose a challenge when it comes to anticipating the second and third order effects of an act of self-defense. If in deploying malware in self-defense it is difficult to anticipate the possible consequences of the use of the code, compliance with the principle of proportionality may be complicated*". LOTRIONTE, C. State sovereignty and self-defense in cyber space, op. cit.; p. 895.

767 HOISINGTON, al respecto propone la no exigencia de estos requisitos a los Estados, en determinadas circunstancias:"State survival may depend on an immediate, robust, and aggressive response; therefore international law should not impose an inflexible requirement on states to fully satisfy the traditional necessity requirements when acting in self-defense of vital state interests. (…) the international community should promulgate a list of critical national infrastructure that a state may protect with active defense measures. If the critical infrastructure identified on the list were subjected to a cyberattack, a state could respond in presumptively good-faith selfdefense without first attributing or characterizing the attack to the level of specificity required under the traditional formulation. HOISINGTON, M., Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, op. cit.; p. 453.

768 Legality of the Threat or Use of Nuclear Weapons, doc. cit.; par. 41 y 42.

Esta decisión, a la que tantas veces se ha hecho referencia, no puede quedar en este punto olvidada, pues nos encontramos ante una situación jurídica, que en el presente puede ser asimilable a la que llevó, en su día, al planteamiento de la cuestión ante la CIJ. Este nuevo método de combate suscita una serie de incógnitas que, como ya se puso de manifiesto al analizar la naturaleza jurídica de las ciberarmas, han de ser resueltas a la luz de los criterios adoptados en torno a otros métodos de combate que, en su momento, han planteado las mismas cuestiones.

De forma evidente, cuando en el desarrollo de un conflicto armado se ejecuten ciberoperaciones, la exigencia de la proporcionalidad que haya de constatarse en la respuesta dada en legítima defensa variará, en función del contexto en el que se presente. Cuando se desarrolle una ciberguerra, probablemente será más sencillo vislumbrar de qué modo la respuesta puede ser proporcional al ataque, al haber identidad de métodos. Si a través de una ciberoperación se destruye un objetivo militar, como un centro de comunicaciones o se inutilizan determinados sistemas de armas, parece evidente que la respuesta haya de circunscribirse a detener ese ataque y, en última instancia, inutilizar el sistema desde el que se lanza. De esta manera, la agresión podrá tomarse como una indicación sobre la medida de la respuesta. Cuando no intervengan métodos de combate más allá de los cibernéticos, habrá que estar a la naturaleza del objetivo y los daños que con la respuesta se consigan.

Como afirma la propia CDI, "*Es muy posible que la acción necesaria para detener y repeler la agresión deba adquirir proporciones que no correspondan a las de la agresión sufrida. Lo que cuenta a este respecto es el resultado que debe alcanzarse mediante la acción «defensiva» y no las formas, la sustancia y la intensidad de la acción misma*[769]". Es decir parece que, en este caso y, *a priori*, el cálculo podría resultar más sencillo. Sin embargo, ya se hizo notar cómo el combate por medios

769Adición al octavo informe sobre la responsabilidad de los Estados, por el Sr. Roberto Ago, Relator Especial, El hecho internacionalmente ilícito del Estado como fuente de responsabilidad internacional (conclusión). Anuario de la Comisión de Derecho Internacional, 1982, vol. II., 1ª parte. Doc. A/CN.4/318/ADD.5 a 7; par. 121.

estrictamente cibernéticos, encuentra sus detractores entre quienes lo consideran poco efectivo.

En la determinación de la proporcionalidad necesaria jugará, asimismo, un papel fundamental, el criterio, anteriormente examinado, de la necesidad de distinguir entre objetivos civiles y militares. Este concepto, que se exponía al tratar el contenido de la obligación internacional violada, cobra aquí, si cabe, mayor importancia pues, como expone REGUEIRO DUBRA, constituye un elemento "*para evaluar el cumplimiento de la necesidad y la proporcionalidad*" [770]

Será, por lo tanto, más usual el supuesto en que se den ciberoperaciones lanzadas en el contexto de una guerra, que podríamos llamar convencional. En estos casos, la proporcionalidad deberá ser calculada en función de diversos factores. En primer lugar, por el criterio de la necesidad. El hecho de que la legítima defensa suponga una autorización del uso de la fuerza no podrá confundirse con una posibilidad sin límites. Antes bien, esta excepcionalidad deberá ser tenida siempre en cuenta, de modo tal que únicamente cuando sea imprescindible deberá recurrirse a ella. Esta excepcionalidad ha sido justificada asimismo, por la CDI que, el documento relativo a la Adición al octavo informe sobre la responsabilidad de los Estados, presentado por el Relator AGO[771], ya estableció que

> "La premisa absolutamente indispensable para que la idea de legítima defensa, en su sentido propio, pueda tener cabida en un sistema de derecho determinado es que ese sistema haya establecido, como norma general, la prohibición del empleo de la fuerza indiscriminadamente por sujetos particulares y no tolere en lo sucesivo ese empleo más que en los casos en que tenga finalidades estrictamente defensivas, es decir, en que adopte la forma de oposición a un ataque violento de otro sujeto. En otros

770 La autora entiende que "En el asunot de las Plataformas Petroliferas (2003), la Corte recordó su jurisprudencia anterior, haciendo hincapié en que la naturaleza civil o militar del objetivo contra el que se usa la fuerza armada en legitima defensa es un criterio para evaluar el cumplimiento de la necesidad y la proporcionalidad". REGUEIRO DUBRA. R. La aportación de la Corte Internacional de Justicia al concepto de legítima defensa. El arreglo pacífico de controversias internacionales. VAZQUEZ GOMEZ, E.M.; ADAM MUÑOS, M.D.; CORNAGO PRIETO, N. (Coordinadores). Tirant lo Blanch. Valencia. 2013; pp. 185 a 204, en particular, p. 191.

771 Adición al octavo informe sobre la responsabilidad de los Estados, por el Sr. Roberto Ago, Relator Especial, El hecho internacionalmente ilícito del Estado como fuente de responsabilidad internacional (conclusión), doc, cit.; par. 83.

términos, la legítima defensa debe considerarse como una causa excepcional de exclusión de la ilicitud de un comportamiento no conforme a una obligación general de no recurrir a la fuerza y, como tal, no tendría sentido concebir su aplicación en un sistema de derecho en el que no existiera tal obligación".

Una ciberoperación, en ocasiones, podrá ser anulada a través de otro ataque informático, que no implique el uso de la fuerza, pero sea suficiente para detener el ataque que se sufre. En dichos supuestos, acudir a la fuerza resultará desproporcionado y, por lo tanto, contrario a la Carta de Naciones Unidas. Sin embargo, cuando un ataque armado, en el desarrollo del combate únicamente pueda detenerse a través de la fuerza armada, sea ésta convencional o cibernética, la respuesta será legítima. En los casos que se ha ido exponiendo a lo largo de la presente tesis, no cabe duda de que la respuesta a través de la fuerza hubiera sido contraria al requisito de la proporcionalidad. El supuesto de los ataques sufridos por Estonia, en modo alguno pudo requerir tal respuesta. Antes bien, en tal caso u otro de similares características, podría haberse reaccionado, inutilizando los servidores desde los que se lanzaban los DDoS o se manipulaban las páginas web. Asimismo, no puede olvidarse que, ante la ilicitud de una conducta por parte de un Estado, el Estado agredido podrá hacer uso de medidas sancionadoras, que no impliquen, necesariamente, el uso de la fuerza.

No obstante, si en el transcurso de un conflicto convencional, como el de Georgia, que también ha sido analizado, una ciberoperación, hubiera dado lugar a un uso de la fuerza ilegítimo, nada hubiera impedido que, a través de métodos de combate convencionales, se anulara dicha posibilidad, por ejemplo, destruyendo el centro de comunicaciones desde el que se lanzaran los mismos.

Por último, la respuesta ante ciberataques que no constituyan métodos de combate, en el sentido que se viene analizando a lo largo de este trabajo, impedirá la respuesta en legítima defensa. Si el ataque no puede atribuirse a un Estado o si el Estado víctima no se halla en conflicto armado o el ataque cibernético no alcanza la magnitud suficiente para tenerlo por ataque armado, la respuesta en legítima defensa no tendrá cabida. Cualquier iniciativa de un Estado

en ese sentido, caerá de lleno en la calificación jurídica que ya se ha dado en el supuesto del virus Stuxnet, pues, ante la falta de agresión, no se puede invocar el derecho a defenderse.

A pesar de que el estudio que aquí se realiza impide un análisis pormenorizado de esta cuestión, en el ámbito estrictamente militar, no puede dejar de mencionarse que, en la invocación del derecho a la legítima defensa, cobra una especial relevancia la posibilidad de acudir a la defensa colectiva, prevista en el artículo 5 del Tratado de OTAN.

El aludido Tratado establece que un ataque armado contra una o más de las Partes del mismo, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas. En consecuencia, si tal ataque se produce, cada una de las Partes, en ejercicio del derecho de legítima defensa individual o colectiva, se comprometen a ayudar a la Parte o Partes atacadas. Seguidamente, de forma individual y de acuerdo con las otras Partes, se adoptarán las medidas que juzguen necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán, inmediatamente, puestas en conocimiento del Consejo de Seguridad de las Naciones Unidas. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales.

A la luz de los criterios hasta ahora expuestos, es factible, por lo tanto, atribuir a un ciberataque la calificación jurídica de ataque armado. En el examen del Tratado de la OTAN resulta obligado hacer referencia a la definición que realiza el artículo 6 del Tratado que, expresamente, considera ataque armado contra una o varias de las Partes, el que se produzca

> "(…) contra el territorio de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer, así como el que se produzca contra las fuerzas, buques o aeronaves de cualquiera de las Partes que se hallen en estos territorios, o en cualquier

otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes, en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer."

En el caso de que el acto de agresión fuera sufrido por uno de los Estados miembros del Tratado OTAN, cada una de las Partes, "*asistirá a la Parte o Partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada para restablecer y mantener la seguridad en la región del Atlántico Norte.*"[772]

De esta manera, cuando ese ataque armado se produzca a través de un ciberataque, no cabe duda de que el reseñado artículo deberá entrar en juego. Bien es cierto que tal medida ha de contemplarse de forma si no excepcional si, al menos, subsidiaria, en el sentido de que el uso de la fuerza armada, como se viene afirmando, ha de ser el último de los recursos para el restablecimiento de la situación y detención de la agresión. No obstante, la aplicación de este artículo, en modo alguno, constituiría una novedad, pues los atentados terroristas sufridos por Estados Unidos en su territorio, en el año 2001, tuvieron como consecuencia la invocación del citado artículo 5[773].

En el caso de una agresión a través de medios cibernéticos, la identificación del agresor y, por lo tanto, la dificultad de atribución del hecho ilícito no puede ser una causa que impida la activación de esta legítima defensa colectiva, de índole militar. Por una parte, esas mismas dificultades técnicas deberían abocar a una mayor cooperación entre Estados, como también se puso de manifiesto en su momento, sin olvidar que dicha cooperación puede llegar a suponer, en un momento dado, la defensa colectiva del Estado agredido. Por otro lado, la asimilación de internet a un método de combate conlleva, necesariamente, la previsión de que, bien la agresión, bien la respuesta puede

772 Artículo 5 del Tratado de OTAN.

773 Por parte de la OTAN, por primera vez en su historia se activó el artículo 5 de su tratado constitutivo, según el cual un ataque contra un Estado integrante de la Alianza es considerado como un ataque contra los demás Estados miembros, los cuales quedan por tanto obligados a prestar asistencia al aliado atacado. EYMAR ALONSO, C., Estados Unidos y la cuestión de la legítima defensa preventiva, doc, cit.

darse por medios cibernéticos[774].

En este punto, hay que resaltar el hecho de que el recurso a la legítima defensa colectiva podría conllevar, desde un punto de vista operativo, la consecuencia de que determinados Estados descuidaran la implantación o actualización de sus capacidades cibernéticas[775]. Así, es necesario reiterar la necesidad de que los Estados proporcionen ya no sólo los medios necesarios, a quienes corresponda la responsabilidad de dirigir ciberoperaciones, sino el adecuado adiestramiento técnico y jurídico, para ello.

En los casos que hasta ahora se han estado exponiendo, los ciberataques sufridos no revistieron entidad suficiente para ser considerados ataques armados y, en consecuencia, la opción de ejercer una legítima defensa colectiva, al amparo del artículo 5 del Tratado OTAN no llegó a plantearse formalmente, aunque siempre se tuvo presente la necesidad de colaboración de los Estados Parte del

774 En este sentido el Manual de Tallin, no ofrece duda en cuanto a la aceptación de la legítima defensa individual y colectiva, en relación con los ciberataques, de manera que a través de la Norma 16, sus autores se muestran partidarios de la aplicación de la legítima defensa colectiva, en los siguientes términos: "*1. The right to collective self-defence authorizes a State or multiple States to come to the assistance of another State that is the victim of an armed attack. This right, explicitly set forth in Article 51 of the United Nations Charter, reflects customary international law. 2. Before a State may come to the assistance of another State in collective self-defence, it must have received a request for such assistance from the victim of the armed attack. Both the victim-State and the State providing assistance must be satisfied that there is an imminent (Rule 15) or on-going armed attack. There is no rule in customary international law permitting one State to engage in collective self-defence of another State solely on the basis of the former's own assessment of the situation. 3. When a State exercises collective self-defence on behalf of another State, it must do so within the scope of the other's request and consent. In other words, the right to engage in collective self-defence is subject to the conditions and limitations set by the victim-State. That State may, for instance, limit the assistance to non-kinetic measures or to passive rather than active cyber defences. 4. Collective self-defence may be exercised either on the basis of a previously concluded collective defence treaty or an ad hoc arrangement. (…) 5. The requirements of necessity, proportionality, imminence, and immediacy (Rules 14 and 15) apply to collective self-defence*". SCHMITT, M.N. (General Editor). Tallin Manual, op.cit; pp. 63 y 64.

775 Así lo ponen de manifiesto COLOM PIELLA y RODRIGUEZ CHIRINO, cuando exponen que ya en octubre del año 2013, la OTAN "*recordó a los veintiocho que las capacidades de ciberdefensa aliadas cubren las necesidades operativas del Cuartel General, la Estructura de Mandos y sus organismos asociados, estando a disposición de los aliados solamente en caso de necesidad. En 2014, se aprobó la tercera Política de Ciberdefensa que, avalada políticamente en la Cumbre de Gales, actualmente se halla en proceso de implementación. Durante este encuentro y, en línea con los planteamientos del Concepto Estratégico 2010, los Jefes de Estado o de Gobierno ratificaron que la ciberdefensa es uno de los principales elementos de la defensa colectiva, siendo también importante en las otras dos core tasks de la OTAN: gestión de crisis y la seguridad cooperativa*". COLOM PIELLA, G y RODRÍGUEZ CHIRINO, C. Construyendo la Ciberdefensa Aliada. Revista de Aeronáutica y Astronáutica. Noviembre 2016; pp. 926-931, en particular, p. 928.

Tratado[776]. Sin embargo, estos precedentes han de tomarse como referencia ilustrativa de la necesidad de que los Estados tengan presente la posibilidad de tener que defenderse colectivamente[777]. En ese caso, se deberá contemplar que, los requisitos y límites de esta acción defensiva no difieren, en nada, de los requeridos para ejercer la legítima defensa individual, que han sido expuestos. Pero, además, como señala SÁNCHEZ RODRÍGUEZ, hay que atender a las particularidades que, en esta modalidad, se manifiestan. La legítima defensa colectiva exige "*que el Estado en beneficio del cual se ejerce este derecho se declare víctima del ataque armado*" y que, además, se formule "*una solicitud por parte del Estado víctima del ataque alegado*", sin olvidar que, en el supuesto de la activación de la defensa colectiva en el marco de la OTAN, se reconozca que dicho Tratado está supeditado "*a las condiciones y requisitos de la Carta, tal y como exige su artículo 103*[778]".

Asimismo, estos requisitos predicables de la legítima defensa colectiva han sido exigidos por la Jurisprudencia Internacional que ha tenido ocasión de señalarlos, con ocasión de la Sentencia relativa a las actividades en Nicaragua[779]. En esta decisión la CIJ estableció que,

> "It is also clear that it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked. There is no rule in customary international law permitting another State to exercise the right of collective self-defence on the basis of its own assessment of the situation. Where collective self-defence is invoked, it is to be expected that the State for whose benefit this right is used will have declared itself to be the victim of an armed attack".

776 Así quedó reflejado, al menos en la prensa que se hizo eco de los relatados hechos: http://news.bbc.co.uk/2/hi/europe/6665195.stm 18/05/2011

777 Una de las consecuencias de los ciberataques sufridos por las repúblicas bálticas en la década del 2000, fue la creación del Centro de Excelencia de OTAN de Ciberdefensa al que se ha hecho alusión en otros apartados del presente trabajo, ubicado geográficamente en Tallin, Estonia. La naturaleza, composición, organización, funciones y documentación publicada por el centro puede ser consultada a través de su página web: http/ccdcoe.org.

778 SÁNCHEZ RODRÍGUEZ, L.I., *Una cara oscura del Derecho Internacional: Legítima defensa y terrorismo internacional*. Cursos de Derecho Internacional de Vitoria-Gasteiz, 2002; pp. 271-299, en particular, pp. 281 y 282.

779 Military and Paramilitary Activities in and against Nicaragua, doc.cit.; par. 197.

Finalmente, puede afirmarse con CASANOVAS Y LA ROSA que, en el ámbito militar, el ejercicio de la legítima defensa colectiva cobra una especial relevancia pues, "*puede entenderse como la respuesta colectiva ante un ataque armado de un estado dirigido contra varios Estados o bien, como la defensa por uno o mas Estados de otro Estado víctima de un ataque armado, no porque los primeros hayan sido también agredidos, sino basada en el interés general de que se mantengan la paz y la seguridad internacionales*[780]".

3. OTRAS CAUSAS QUE EXCLUYEN LA ILICITUD.

Para abordar el segundo de los objetivos específicos del presente trabajo resulta necesario atender a las cuestiones relativas a las causas que excluyen la ilicitud. Sin perjuicio de la preponderancia de la legítima defensa, por los motivos que han quedado expuestos, es necesario examinar el resto de las circunstancias contenidas en el Proyecto de artículos. Se tratará, nuevamente, de examinar si estas circunstancias, expresivas de valores superiores a los lesionados por el hecho ilícito, resultan condicionadas por la introducción del elemento cibernético.

3.1. El consentimiento prestado por el Estado durante el conflicto armado.

El artículo 20 del Proyecto de artículos contempla, como la primera de las causas de justificación del hecho ilícito, que éste haya sido consentido por el Estado agredido y, al respecto, establece que

> "El consentimiento válido de un Estado a la comisión por otro Estado de un hecho determinado excluye la ilicitud de tal hecho en relación con el primer Estado en la medida en que el hecho permanece dentro de los límites de dicho consentimiento".

Este consentimiento se configura de forma amplia, pues abarca, prácticamente, cualquier situación que pueda originarse en Derecho

780 CASANOVAS Y LA ROSA, O. *El principio de prohibición del uso de la fuerza*, op. cit.; p. 1075.

Internacional[781], siempre que la aquiescencia del Estado sea válida y en "*la medida en que el hecho permanece dentro de los límites de dicho consentimiento*".

Del texto del citado artículo pudiera interpretarse que, únicamente, las excepciones contempladas en el artículo 26 constituyen casos en los que el consentimiento del Estado resulta inválido. Es decir, reuniendo los requisitos de validez descritos en el artículo 20, en principio, podría otorgarse el consentimiento del Estado a todos los hechos ilícitos, salvo aquéllos que se produjeran como consecuencia de la violación de una norma imperativa, en los términos vistos más arriba. Es decir que, este consentimiento puede ser entendido como la expresión máxima de la soberanía del Estado en la que las obligaciones jurídicas internacionales han de basarse, de modo que, únicamente, en aquellas obligaciones en las que dicha disponibilidad no puede entrar en juego, quedaría excluida la eficacia del consentimiento.

Pues bien, con carácter previo es necesario realizar una aproximación a la licitud del consentimiento y, de este modo, hay que traer de nuevo a colación el concreto contenido de las normas de DIH que ha sido expuesto previamente, para determinar si es posible o no que por parte del Estado se consienta en la infracción.

En primer término, hay que recordar que las obligaciones cuyo concreto contenido ya ha sido examinado, no son, en su mayor parte, disponibles por del Estado. En el concreto caso que aquí se examina en el que el Estado agredido se encuentra librando una ciberguerra o un conflicto convencional, su consentimiento se verá sometido a unas circunstancias muy específicas. Es decir, la situación de conflicto bélico podrá determinar que el Estado transgresor se vea impedido para el cumplimiento de ciertas obligaciones internacionales anteriormente contraídas. En ese caso, el consentimiento del Estado lesionado, vinculado jurídicamente al Estado que ahora no puede cumplir con su obligación, impediría el nacimiento de responsabilidad internacional. Podría ser el caso, por ejemplo, de un Estado en conflicto que no se encontrara en situación de llevar a término ciertas obligaciones comerciales o de índole económica. En un

781 Así puede desprenderse del contenido del Comentario 2) al artículo 20.

supuesto así, el Estado frente al que no se cumplen dichas obligaciones, en uso de su soberanía y del mantenimiento de sus relaciones internacionales, podría otorgar su válido consentimiento a este incumplimiento y declinar, así, el ejercicio de cualquier acción para exigir la correspondiente responsabilidad internacional.

Sin embargo, el propio conflicto armado conllevará la presencia de muchas otras obligaciones internacionales, inherentes al mismo, en las que el consentimiento del Estado será crucial. Es el caso, por ejemplo, del establecimiento de tropas extranjeras en el territorio nacional. Este supuesto, frecuente en la actualidad supone que bien, actuando a través de Organizaciones Internacionales, bien en coaliciones de Estados, las Fuerzas Armadas de varios Estados se establecen físicamente en el terreno de un tercero. Esta situación, desde el punto de vista el Derecho Internacional ha sido tradicionalmente articulada, a través de la prestación del consentimiento del Estado, que recibe dichas tropas. Se trata, así de un modo de actuación, en las relaciones internacionales que ha dado lugar a una serie de Convenios internacionales que, bajo el acrónimo de SOFA ha permitido la prestación de ese consentimiento estatal, cuya ausencia, originaría la ilícita invasión de un Estado extranjero. De este modo, la gran parte de las Organizaciones Internacionales[782], cuentan con un modelo de Estatuto que, asumido por el Estado receptor, recoge el régimen jurídico del personal y del material militar desplazados a territorio extranjero.

En este sentido, hay que recordar que dicho consentimiento deberá ser

782 El SOFA de la OTAN es un Tratado Internacional, que ha sido incorporado al Derecho interno español, a través del Instrumento de Adhesión de España al Convenio entre los Estados Partes del Tratado del Atlántico Norte relativo al Estatuto de sus Fuerzas, hecho en Londres el 19 de junio de 1951, publicado en el BOE de 10 de septiembre de 1987. De forma semejante, la UE cuenta con su propio estatuto, aplicable a las tropas que, bajo su mandato, se establezcan en territorio extranjero, a través del "Agreement between the Member States of the European Union concerning the status of military and civilian staff seconded to the institutions of the European Union, of the headquarters and forces which may be made available to the European Union in the context of the preparation and execution of the tasks referred to in Article 17(2) of the Treaty on European Union, including exercises, and of the military and civilian staff of the Member States put at the disposal of the European Union to act in this context (EU SOFA) (2003/C 321/02)", publicado en el Diario Oficial de la Unión Europea, de 21 de diciembre de 2003. Por último, la Organización de Naciones Unidas cuenta con el Proyecto de Modelo de Acuerdo sobre el Estatuto de las Fuerzas entre las Naciones Unidas y los Países Receptores, recogido en el Documento de la Asamblea General Doc. /A/45/459, de 9 de octubre de 1990.

prestado por el Estado o un quien actúe en su nombre pues, como pone de manifiesto el Comentario al Proyecto de artículos, el consentimiento prestado por un agente de un gobierno regional, puede ser válido para atribuir la conducta al Estado, pero no para eximir al mismo de su responsabilidad internacional, al no tratarse de una autoridad legitimada[783].

El consentimiento, además, debe ser libre y "*haberse manifestado claramente y ser expresado efectivamente por el Estado y no sólo presumido sobre la base de que el Estado habría dado su consentimiento si se le hubiera pedido*"[784]. Al igual que ocurre en la prestación del consentimiento por el Estado cuando el mismo pretende establecer vínculos, cuando ese mismo Estado consiente la realización de un hecho ilícito, es preciso que su consentimiento no se encuentre viciado. Se tratará en estos casos de ilícitos por acción u omisión respecto de los que no podrá exigirse responsabilidad internacional al Estado que los cometa, por cuanto el Estado receptor consiente válidamente en que el hecho se produzca. En estos supuestos, la licitud del consentimiento se presenta vital pues, ciertamente del mismo no se derivan obligaciones como pudiera ocurrir en situaciones más frecuentes, pero impedirá el surgimiento de una obligación internacional, que es la propia de la responsabilidad del Estado infractor. En consecuencia, no quedará eximido de su responsabilidad internacional el Estado que haya prestado su consentimiento por error, fraude, corrupción o coacción.

En definitiva, en el desarrollo del conflicto armado, podrá darse el consentimiento válido del Estado, en los términos hasta ahora expuestos. Cuestión distinta será, sin embargo, la aceptación de hechos ilícitos que contravengan el DIH. Es decir, no podrá darse el caso de que el Estado preste su consentimiento para que otro Estado o agente no estatal infrinja, de tal modo el DIH, que incurra en alguna de las prohibiciones enumeradas, anteriormente. Dicha indisponibilidad se justifica en el hecho de que, como se acaba de señalar en el epígrafe anterior, determinadas normas de DIH podeen naturaleza de *ius cogens* y, por lo tanto, quedan sujetas a la indisponibilidad que ya ha sido

783 Comentario 5) al artículo 20 del Proyecto de artículos.
784 Así puede leerse en el Comentario 8) al artículo 20 del Proyecto de artículos.

examinada.

En el caso español las normas de DIH resultan exigibles, además, en virtud del ordenamiento jurídico interno, de manera tal que, con independencia del resto de los requisitos necesarios para otorgar validez al consentimiento del Estado, en el caso de determinadas violaciones de DIH, la aquiescencia del mismo, contravendría también el Derecho Penal[785]. El consentimiento en relación a una ciberoperación que constituyera una violación grave y a gran escala de una de las obligaciones antes vistas, es decirm que careciera de necesidad militar o que no respetara la distinción entre objetivos civiles o militares o cualquier otra de las enumeradas más arriba, tendría como consecuencia la comisión del correspondiente delito recogido en el Capítulo III del Título XXIV del Código Penal, que recoge los delitos contra las personas y bienes protegidos en caso de conflicto armado[786].

En consecuencia, es evidente que no puede otorgarse la misma validez a cualquier manifestación de voluntad prestada por el Estado, pues si bien, durante el conflicto armado, el consentimiento estatal será válido para justificar un ilícito internacional, sin embargo, la observancia de las normas de DIH aplicables al combate será indisponible.

3.2. Las contramedidas y su relación con las represalias bélicas.

La siguiente causa de exención de la ilicitud de la conducta, que se prevé en el Proyecto, con carácter general, es la contenida en el artículo 22, que establece:

"La ilicitud del hecho de un Estado que no esté en conformidad con

785 El artículo 46 del Convenio de Viena sobre los Tratados, al respecto establece que "*1. El hecho de que el consentimiento de un Estado en obligarse por un tratado haya sido manifiesto en violación de una disposición de su derecho interno concerniente a la competencia para celebrar tratados no podrá ser alegado por dicho Estado como vicio de su consentimiento, a menos que esa violación sea manifiesta y afecte a una norma de importancia fundamental de su derecho interno. 2. Una violación es manifiesta si resulta objetivamente evidente para cualquier Estado que proceda en la materia conforme a la práctica usual y de buena fe*".

786 Los artículos 608 a 616 bis) del Codigo Penal recogen, esencialmente, las conductas que han sido enumeradas con ocasión del análisis del artículo 8 del estatuto de la Corte Penal Internacional.

una obligación internacional suya para con otro Estado queda excluida en el caso y en la medida en que ese hecho constituya una contramedida tomada contra ese otro Estado de conformidad con el capítulo II de la tercera parte".

El presente artículo se limita a definir y enunciar las contramedidas que se encuentran reguladas, de forma detallada, en el Capítulo II de la Tercera Parte del Proyecto. Así, serán los artículos 49 a 53 del mismo documento los que fijen las condiciones en que pueden establecerse dichas contramedidas. La presencia de contramedidas, esencialmente, supone que, ante la comisión por un Estado de un hecho internacionalmente ilícito, el Estado lesionado podrá adoptar dichas contramedidas, a fin de lograr su cesación y obtener reparación por el daño sufrido y, siempre y cuando, no entrañen el uso de la fuerza[787].

El artículo 22 trata esta situación desde la perspectiva de las circunstancias que excluyen la ilicitud, mientras que, el Capítulo II, por su parte, establece las condiciones bajo las que las contramedidas pueden justificar un comportamiento que, en otro caso sería ilícito, pero que "*deben adoptarse en respuesta a un hecho internacionalmente ilícito cometido, anteriormente, por otro Estado y estar dirigidas contra ese Estado*[788]".

En este punto, habida cuenta el concreto aspecto que aquí se analiza, habrá que plantearse si la violación de una norma de DIH, utilizando un ciberataque como método de combate puede ser admitido pues, como ha quedado expuesto, las contramedidas no admiten el uso de la fuerza. En consecuencia, es necesario ahora detenerse en el examen de lo que podrían ser las contramedidas en el combate, es decir, las represalias bélicas. No puede olvidarse que el hecho ilícito, que aquí se examina, consiste en la violación de normas relativas al combate, por lo cual, las represalias que se contienen en el Proyecto, podrían darse para cualquier Estado que, en situación de conflicto armado, sufriera la violación de una obligación internacional, siempre y cuando ésta no sea relativa al propio combate.

787 "*State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State*". SCHMITT, M.N. (General Editor). Tallin Manual, op.cit.; p.41.
788 Comentario 2) al artículo 22 del Proyecto de artículos.

Por lo tanto, en el examen de las infracciones de DIH que se produzcan durante el combate y el modo en que el DIH ha de hacerse respetar habrá aque acudir, nuevamente, a la Compilación de DIH Consuetudinario que prevé, en su Norma 145, la posibilidad de represalias bélicas[789]. Es decir, que en el transcurso del combate, la violación de una norma de DIH conllevará, en su caso y, con las limitaciones que ahora se verán, la adopción de represalias y no de contramedidas[790]. En este sentido, ninguna duda ofrece la posibilidad de que se adopten dichas represalias pues, como señala CARDONA LLORENS "*La licitud de las represalias armadas, como respuesta a la comisión por otro Estado, de un hecho ilícito internacional previo en general, es sostenida por la mayoría de la sociedad internacional contemporánea y por la mayoría de la doctrina*".[791]

Sin embargo, el artículo 50 del Proyecto pone de manifiesto una prohibición que, de modo general se contiene en el DIH Convencional y Consuetudinario, relativa a la adopción de represalias contra personas y que también es recogida en los Convenios de Ginebra y en su PA I, donde se establece que "*se prohíben las represalias contra determinadas clases de personas protegidas y estas prohibiciones gozan de una aceptación muy amplia*[792]". Asimismo, la aludida norma 145 especifica que dichas represalias podrán adoptase "*cuando no están prohibidas por el Derecho Internacional*" siendo ésta pues, la principal restricción[793]. Adicionalmente, la Compilación de DIH Consuetudinario entiende exigibles cinco condiciones que las represalias han de cumplir, para ser consideradas lícitas.

789 Así se desprende del texto del artículo 50.1 del Proyecto que establece: "Las contramedidas no afectarán: a) La obligación de abstenerse de recurrir a la amenaza o al *uso de la fuerza*, como está enunciada en la Carta de las Naciones Unidas; b) Las obligaciones establecidas para la protección de los derechos humanos fundamentales; c) Las obligaciones de carácter humanitario que prohíben las represalias; d) Otras obligaciones que emanan de normas imperativas del derecho internacional general".

790 A tenor de la citada Compilación "*Una represalia bélica consiste en una acción que, en otras circunstancias, sería ilícita, pero que, en casos excepcionales, se considera legítima con arreglo al derecho internacional cuando se emplea como medida coercitiva en respuesta a actos ilícitos de un adversario*". HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p. 580.

791 GUTIERREZ ESPADA, *La responsabilidad internacional del Estado por el uso de la fuerza armada (la conformación del hecho ilícito internacional)*, op.cit.; p. 301.

792 Así puede leerse en el Comentario 8) al artículo 50 del Proyecto.

793 De la misma forma, el Proyecto, en el párrafo 1 de su artículo 50, impide la adopción de represalias ilegales, teniendo por ésta las que están prohibidas por el DIH.

La primera de ellas supone que la represalia sea adoptada, "*en respuesta a una violación grave del derecho internacional humanitario cometida con anterioridad, y únicamente con el fin de inducir al adversario a respetar el derecho*". A la vista del enunciado de este primer requisito y, teniendo en cuenta que los cuatro posteriores han de darse de forma acumulativa a éste y no alternativa, se alcanza a comprender la falta de uso de esta medida por parte de los Estados[794]. Se trata por lo tanto, de limitar el uso de las represalias a violaciones graves y previas, sin que tampoco aquí quepa el concepto de anticipación que será examinado con mayor detenimiento al analizar los requisitos de la legítima defensa. En cualquier caso, la Compilación vuelve a dirigir nuestro estudio a las violaciones graves que han sido ya examinadas.

Si hay algo que vuelve a ponerse nítidamente de manifiesto es que, el Proyecto salvaguarda la obligación de abstenerse de *recurrir a la amenaza o al uso de la fuerza,* tal y como prevé la Carta de las Naciones Unidas.

Por lo tanto, nos encontramos con una importantísima excepción a dicha prohibición, únicamente justificada por el hecho de haber sido víctima de una violación grave de las normas de DIH. Ya hemos hecho referencia a la situación en que puede hallarse un Estado en conflicto y al hecho de que pueden producirse otras violaciones de obligaciones internacionales, al margen de las contenidas en el DIH. Pues bien, puesto que estas contramedidas contempladas en el Proyecto, en modo alguno permitirán el uso de la fuerza, el recurso al mismo se limitará a la respuesta a una violación grave del DIH, revistiendo entonces los caracteres de represalias, con todas sus consecuencias.

Este límite es completado con el resto del enunciado del artículo 50 del Proyecto, cuando establece que tampoco las represalias podrán afectar a "*las obligaciones establecidas para la protección de los derechos humanos fundamentales*"; "*las obligaciones de carácter humanitario que prohíben las represalias*; "*otras obligaciones que*

794 Tal y como puede leerse en la Compilación, "*La renuencia de los Estados a recurrir a las represalias puede explicarse por el hecho de que no son eficaces como medio para hacer cumplir el derecho, en particular porque conllevan el riesgo de una escalada de las violaciones. Indican que la comunidad internacional se opone cada vez más al recurso a violaciones del derecho internacional humanitario como método para hacer respetar el derecho*". HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op.cit.; p. 582.

emanan de normas imperativas del derecho internacional general".

Por lo tanto, resulta evidente el específico régimen jurídico que emana de la previsión de las represalias en este específico ámbito. Así, será a esta regulación a la que haya de acudirse en relación con la violación de las normas de DIH antes examinadas, habida cuenta su doble condición de "*obligaciones de carácter humanitario*", emanadas de "*normas imperativas del derecho internacional general*".

Así, en segundo lugar, las represalias bélicas han de constituir un último recurso, en aras a hacer respetar el DIH[795], "*cuando no se dispone de otras medidas lícitas para inducir al adversario a respetar el derecho*". Es decir, cuando el DIH permite el uso de la fuerza, en respuesta al hecho ilícito, la licitud del mismo se restringe de modo tal que impide el acuerdo de represalias si existiera otro modo de hacer cumplir el DIH, incluso en casos en que se haya cometido una violación grave. De forma evidente, dichos requisitos resultan mucho más restrictivos que los contemplados por el Proyecto para la adopción de contramedidas[796].

En tercer lugar, el DIH exige las represalias sean proporcionadas "con respecto a la violación a la que se quiere poner fin". Como se verá, al exponer los requisitos del ejercicio del derecho a la legítima defensa, el requisito de la proporcionalidad será el uno de los que mayor complejidad presenten. En el caso de ciberataques la proporción habrá de guardarse de forma tal que, con independencia de que la ciberoperación constituya una represalia ante una violación grave cometida por métodos convencionales o, viceversa, constituya en sí un crimen frente al que se pretende reaccionar, deberá observarse escrupulosamente este requisito. Serán pues, los bienes jurídicos en juego los que

795 Ibidem, p. 583.

796 Además de la proporcionalidad exigida por el artículo 51 del Proyecto, el artículo 52 establece las siguientes condiciones a las contramedidas: "*1. Antes de tomar contramedidas, el Estado lesionado: a) Requerirá al Estado responsable, de conformidad con el artículo 43, que cumpla las obligaciones que le incumben en virtud de la segunda parte; y b) Notificará al Estado responsable cualquier decisión de tomar contramedidas y ofrecerá negociar con ese Estado. 2. No obstante lo dispuesto en el apartado b) del párrafo 1, el Estado lesionado podrá tomar las contramedidas urgentes que sean necesarias para preservar sus derechos. 3. Las contramedidas no podrán tomarse y, en caso de haberse tomado, deberán suspenderse sin retardo injustificado, si: a) El hecho internacionalmente ilícito ha cesado; y b) La controversia está sometida a una corte o un tribunal facultados para dictar decisiones vinculantes para las partes.4. No se aplicará el párrafo 3 si el Estado responsable no aplica de buena fe los procedimientos de solución de controversias*".

determinen la proporcionalidad de la respuesta, sin que sea lícita la represalia bélica que lesione un bien jurídico superior.

La Compilación de DIH Consuetudinario, al establecer los requisitos de licitud de las represalias bélicas, exige, en cuarto lugar, que las mismas sean consecuencia de la decisión adoptada por quien detente el nivel *más alto del Gobierno.* Advierte así, la Compilación que dicha decisión no puede recaer en manos de "*los jefes militares sobre el terreno*". No puede añadirse aquí sino que, tal limitación resulta consecuente con la excepcionalidad que supone la adopción de dicha decisión. Por este motivo, deberá rechazarse como lícita cualquier medida de este tipo que sea tomada por autoridades de nivel inferior y, en el caso que nos ocupa, siempre por agentes no estatales.

Por ultimo se exige que, una vez en marcha, las represalias cesen tan pronto como el "*adversario respete el derecho*". Una vez más se pone de manifiesto la naturaleza subsidiaria de esta respuesta, que impide el recurso a la fuerza, en el mismo momento que deja de ser necesario para el mantenimiento de la legalidad. Este rasgo es compartido, asimismo, por las contramedidas previstas en el Proyecto, en caso de violación de otras obligaciones internacionales, de modo que en ambos casos puede decirse que nos encontramos ante respuestas que han de limitarse a lo que resulte imprescindible. En concreto, el artículo 52 del Proyecto, exige que las contramedidas sean suspendidas en cuanto "*el hecho internacionalmente ilícito ha cesado*".

En el ámbito del conflicto cibernético, las medidas que, concretamente, puedan adoptarse a modo de represalia, presentarán sus específicas modalidades de orden técnico[797], pero no en cuanto a su régimen jurídico. Sirva aquí como

797 KESAN y HAYES, exponen estas particularidades ofreciendo los siguientes ejemplos: "*In the cyber context, a "counterstrike" can involve a number of actions. It can involve the target redirecting the attacker's packets back at the attacker, executing its own Denial of Service (DoS) attack at the attacker to knock the attacker's systems off-line, infecting the attacker's system with a virus or worm to permit the victim to take control, and a number of other options or combinations of options. Additionally, there is now evidence that "cyber contractors" exist as part of what some have termed the new "military digital complex," whose work involves the creation of offensive cyber technologies that could have application in the context of counterstriking. The goal of a counterstrike can also vary between punishing the attacker or simply mitigating the harm to the target. The former can be termed "retributive counterstriking," which we argue should remain under the sole control of the military as a national security matter at this stage because of the sensitivity of constitutional issues and international law issues. "Mitigative counterstriking," on the other hand, can be defined as active efforts to mitigate harm to a victim system in a*

ejemplo, de nuevo, el supuesto de los ataques que la empresa Sony sufrió, al parecer, por parte del Estado de Corea del Norte. Pues bien, como ya se expuso en otro lugar del presente trabajo, fueron los Estados Unidos los que tomaron la iniciativa en relación a la respuesta que, dichos ataques, a su juicio, pudieron merecer. Toda vez que ninguno de los dos Estados se hallaba inmerso en un conflicto bélico, la violación de una obligación internacional por parte de Corea del Norte pudiera haber sido respondida por los Estados Unidos, a la luz de lo dispuesto en el Proyecto de artículos y, por lo tanto, las medidas tomadas, en ese sentido, podrían haber tenido cabida en las contramedidas aquí estudiadas. Sin embargo, si ello se hubiera producido como consecuencia de una ciberoperación en el transcurso de un conflicto, la valoración de la respuesta hubiera tenido que ser distinta. Únicamente en el caso en que dicho ataque armado cibernético hubiera podido ser conceptuado como la violación de una obligación grave de las normas de DIH, del tenor antes visto, habrían tenido cabida las represalias por parte de los Estados Unidos.

En este sentido, la respuesta ofrecida por los Estados Unidos, hasta donde ha podido conocerse, cumpliría con los requisitos que aquí se recogen, toda vez que fue adoptada, una vez constatado el ataque, observando la proporcionalidad adecuada y por parte del más alto nivel del Gobierno, que asumió el "contraataque" o contramedida, como propia, en nombre de la compañía Sony.

Por otra parte, la adopción de represalias bélicas plantea la cuestión de cuál es el Estado legitimado para hacerlo. Si hemos distinguido entre las contramedidas y las represalias, en función de la obligación internacional violada, no se puede ahora desatender la consecuencia que de ello se deriva, en relación con la legitimación de la respuesta. Conforme al estudio previo, ha de

---

manner that is strictly limited to the amount of force necessary to prevent the victim from being further damaged (…). *mitigative counterstriking must be to mitigate damage from a current and immediate threat, and we urge that whatever measures are deployed must be justifiable under this mitigation framework* (...).*We posit that accurate and consistent use of mitigative counterstrikes could serve to deter certain types of cyberattacks against sensitive systems such as hospitals, government defense systems, and critical national infrastructure (CNI), and urge that implementing a regime to permit these sorts of counterstrikes should be a priority. (…). We thus propose a new policy and legal regime to address the threat of cyberattacks through the use of "active defense" and "mitigative counterstriking*". KESAN, J. P. and HAYES, C. M. *Self Defense in Cyberspace: Law and Policy,* op. cit.; pp.3-5.

afirmarse que las contramedidas han de ser adoptadas por el Estado víctima, atendiendo los criterios arriba expuestos. En este sentido se había pronunciado ya la CIJ en su Sentencia relativa a las actividades militares y paramilitares en Nicaragua[798]. En su pronunciamiento, la Corte distingue entre la legitimidad de la adopción de contramedidas, encaminadas a detener un hecho ilícito de menor gravedad que un ataque armado, y la legítima defensa colectiva que se justificaría en el caso de que dicho ataque armado se produjera, restringiendo la primera posibilidad únicamente al Estado víctima.

En relación con lo anterior, no puede olvidarse que la violación de una norma imperativa conllevará, asimismo, la exigencia de responsabilidad internacional, conforme a lo dispuesto en el Proyecto que, en su artículo 48, prevé que "*Todo Estado que no sea un Estado lesionado tendrá derecho a invocar la responsabilidad de otro Estado de conformidad con el párrafo 2 si: (…) b) La obligación violada existe con relación a la comunidad internacional en su conjunto.*" En consecuencia, la exigencia de responsabilidad internacional se extiende a, en virtud del apartado 2 del mismo artículo a la "*cesación del hecho internacionalmente ilícito y las seguridades y garantías de no repetición*" y al "*cumplimiento de la obligación de reparación (…) en interés del Estado lesionado o de los beneficiarios de la obligación violada*".

De esta manera, una vez se ha concluido que las normas de *ius cogens* son aquellas que vinculan a la Comunidad Internacional, en su conjunto, cabría la posibilidad que esa Comunidad Internacional se sintiera legitimada para ofrecer una respuesta. En el caso que nos ocupa, la violación de una norma de DIH durante el combate, en las condiciones que han sido expuestas, podría, pues, legitimar la adopción no sólo de la legítima defensa colectiva, que se estudiará

798 Así se expresa la Corte, al afirmar que "*On the legal level the Court cannot regard response to an intervention by Nicaragua as such a justification. While an armed attack would give rise to an entitlement to collective self-defence, a use of force of a lesser degree of gravity cannot, as the Court has already observed (paragraph 211 above), produce any entitlement to take collective countermeasures involving the use of force. The acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts, namely El Salvador, Honduras or Costa Rica. They could not justify counter-measures taken by a third State, the United States, and particularly could not justify intervention involving the use of force*". Military and Paramilitary Activities in and against Nicaragua, doc.cit; par. 249.

más adelante, sino de represalias[799].

Por ultimo, únicamente cabe señalar que, el DIH contempla la prohibición del uso de represalias bélicas, contra las personas y bienes protegidas por los Convenios de Ginebra[800].

3.3. La fuerza mayor.

En virtud de lo dispuesto en el Proyecto de artículos, un hecho ilícito que se origine como consecuencia de una fuerza mayor, impedirá la exigencia de responsabilidad, atendido el texto del artículo 23 que establece,

> "La ilicitud del hecho de un Estado que no esté en conformidad con la obligación internacional de ese Estado queda excluida si ese hecho se debe a una fuerza mayor, es decir, a una fuerza irresistible o un acontecimiento imprevisto ajenos al control del Estado, que hacen materialmente imposible, en las circunstancias del caso, cumplir con la obligación".

En los dos casos enunciados por el Proyecto, resulta determinante que el hecho ilícito se haya producido, como consecuencia de una acción u omisión en la que el Estado no ha tenido ocasión de intervenir. Al respecto, el concepto de fuerza mayor, en relación con la acción u omisión del Estado, no dista del contenido en el Derecho interno y que la Jurisprudencia del ámbito contencioso ha definido, deslindándolo del concepto de caso fortuito, de la siguiente manera:

> "En la fuerza mayor, en cambio, hay determinación irresistible y exterioridad; indeterminación absolutamente irresistible, en primer lugar, es decir aun en el supuesto de que hubiera podido ser prevista;

799 En relación a esta cuestión, puede verse BARBOZA, J., Contramedidas en la reciente codificación de la responsabilidad de los Estados. Fronteras con la legítima defensa y el estado de necesidad. Anuario Argentino de Derecho Internacional, vol. XII, 2003; pp.1-47, en particular, pp. 44-47.

800 Así lo establecen las Normas 146 y 147 de la Compilación de Derecho consuetudinario. HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, op. cit.; pp. 586-594.

> exterioridad, en segundo lugar, lo que es tanto como decir que la causa productora de la lesión ha de ser ajena al servicio y al riesgo que le es propio. En este sentido, por ejemplo, la TS S 23 May. 1986: «Aquellos hechos que, aun siendo previsibles, sean, sin embargo, inevitables, insuperables e irresistibles, siempre que la causa que los motive sea extraña e independiente del sujeto obligado». En análogo sentido: TS S 19 Abr. 1997 (apelación 1075/1992)[801]".

La principal nota característica pues, tal y como señala el Comentario al artículo 23, está constituida por "*la falta de voluntad del Estado en este comportamiento*[802]". Por lo tanto, en estos supuestos será preciso constatar en qué momento y circunstancias, el Estado puede verse completamente imposibilitado para ejercer su voluntad, hasta el punto de cometer la violación de una obligación internacional. En consecuencia, es necesario analizar el modo en que se origina la causa de fuerza mayor, es decir, un acontecimiento natural o físico o bien, una intervención humana.

En el caso de que el Estado se halle en una situación de conflicto armado, el segundo de los casos parece de más probable ejecución. Es decir, como veíamos en los supuestos previos, podrá darse la situación de que, el Estado en conflicto, infrinja una obligación internacional. En un conflicto armado ha de tenerse presente la posibilidad de que el Estado pierda el control del combate, en el sentido de que puede producirse la sedición de una parte de la Fuerza, así como supuestos de rebelión o de insurgentes que toman el control. Si, efectivamente, el ilícito internacional se debiera a la intervención de estas causas, la conducta no podrá reputarse ilícita, a la luz de lo dispuesto en el transcrito artículo 23 del Proyecto. En este caso, nuevamente, hay que recordar la complejidad que los ataques informáticos conllevan en materia de atribución. Por lo tanto, en supuestos como este será necesario probar que, indudablemente, las acciones u omisiones, a través de los que se ha infringido una obligación internacional, por medios de un ciberataque no se deben, en modo alguno, a la conducta del Estado. También en estos casos será necesario, en su momento,

801 Así puede leerse en la Sentencia dictada por la Sala Tercera, de lo Contencioso-administrativo, Sección 6ª del Tribunal Supremo, con fecha de 31 Mayo de 1999.
802 Comentario 1) al artículo 23 del Proyecto de artículos.

descartar completamente, cualquier uso fraudulento de otra identidad que el Estado pudiera realizar, precisamente, pare eludir la responsabilidad internacional.

Sin embargo, si la situación de fuerza mayor "*se debe, únicamente o en combinación con otros factores, al comportamiento del Estado que la invoca*", la actuación del Estado será a todos los efectos ilícita, sin que quepa la justificación contenida en este artículo.

Por otra parte, la fuerza mayor puede deberse a un acontecimiento irresistible y exterior, lo que es tanto como decir que la causa productora de la lesión ha de ser ajena a cualquier conducta humana. En el caso de los ciberataques que violan una obligación internacional, podría darse un fenómeno que causara una disfunción en los sistemas, hasta el punto de que el Estado en cuestión se viera imposibilitado de actuar. Aun cuando pudiera parecer que este hecho resulta improbable, en el ámbito que nos encontramos, hay que poner de manifiesto que ya se han producido situaciones encuadrables en estas circunstancias. Este es el caso de la falta de operatividad constatada en los aeropuertos del Reino Unido, durante la jornada del 12 de diciembre de 2013[803]. Lo que, en principio, podría haberse considerado como ataque a la red, dirigido a provocar el colapso de la navegación aérea británica, con el tiempo se reveló

803 El siguiente extracto del extenso relato de los hechos, recogido en el informe independiente que analizó el incidente, resulta revelador: "*The Incident started with the failure at 1444 UTC (this and all subsequent times are reported in the 24 hour format at UTC) of a computer system used to provide data to Air Traffic Controllers to assist their decision-making when managing the traffic flying at high level over England and Wales. This traffic includes aircraft that have departed or are planned to arrive at major London airports (Heathrow, Gatwick, Stansted, Luton and City) as well as aircraft transiting UK airspace. The Controllers put their pre-agreed operating procedures into action for the particular computer system failure; these included adopting manual methods for decision-making to ensure aircraft continue to maintain safe separation and restricting air traffic entering their area of responsibility. At 1455 all departures were stopped from London Airports and at 1500 all departures were stopped from European airports that were planned to route through affected UK airspace. The engineering experts were able to determine the nature of the failure and agree a safe recovery procedure so that the computer system was restored to the Controllers at 1549, but without its normal level of redundancy (back-up). By 1900, the Engineering staff believed they understood the cause of failure and full redundancy of the computer systems was restored at 2010. Traffic restrictions were gradually lifted from 1555 as confidence increased, and the final restriction was lifted at 2030. The disruption caused by the restrictions affected airlines, airports and passengers into the following day*". NATS System Failure 12 December 2014 – Final Report Independent Enquiry Final Report dated 13 May 2015. Authors: Robert Walmsley, Timothy Anderson, Clay Brendish, John McDermid, Martin Rolfe, Joseph Sultana, Mark Swan, Michael Toms; p. 3.

como un fallo "*occurred […] because of a latent software fault that was present from the 1990s; this is referred to as the proximate cause of the failure*"[804].

En un supuesto como el anterior, el Estado que incurre en la violación de una obligación internacional quedará exento de su responsabilidad si invoca y demuestra que, efectivamente, se hallaba en una situación de fuerza mayor. En los supuestos de ciberataques parece más probable que dicha violación se pueda producir por omisión pues podría suceder que, debido a fenómenos meteorológicos o a la pérdida de control de las comunicaciones por parte del Estado durante el combate, se produzcan violaciones de obligaciones internacionales, de conformidad con lo expuesto, no podrán originar la relación jurídica propia de la responsabilidad internacional.

Nuevamente, aun de forma tangencial, hay que hacer aquí énfasis en la cuestión de la atribución. No procede aquí sino remitir a lo expuesto en el Capítulo correspondiente, en relación a la actuación de agentes no estatales para concluir que, en realidad, la presente causa de exención, se encuentra relacionada de forma más estrecha con la autoría de la acción u omisión que con una causa de exención de la ilicitud. Así, en los demás supuestos nos encontramos ante actuaciones del Estado que constituyen un hecho ilícito, respecto de los que se da una justificación. Sin embargo, en este caso, la primera afirmación no puede ser tenida como válida pues no existe acción u omisión del Estado, toda vez que el hecho no puede serle atribuido. Asimismo, desde esta perspectiva, parece cobra mayor sentido la excepción contenida en el artículo 23 del Proyecto cuando entiende que la causa de exención no puede invocarse cuando la fuerza mayor se deba al comportamiento del Estado, ya se haya producido esta actuación únicamente por el Estado, "*o en combinación con otros factores*".

En consecuencia, podría afirmarse que esta exención de ilicitud entra en juego, no en el momento en que se justifica la ilicitud del hecho, sino cuando no puede realizarse la atribución del mismo al Estado. Por este motivo también es preciso recordar la necesidad de que dicha atribución resulte lo más nítida

804 NATS System Failure 12 December 2014. Final Report, doc. cit.; p. 4.

posible sin que sea deseable asumir las teorías que ya han sido expuestas y que abogan por la adopción de criterios de atribución más laxos.

En aplicación de este mismo razonamiento cobra sentido la segunda de las causas por las que resulta inviable invocar esta causa de justificación: que el Estado haya "*asumido el riesgo de que se produzca esa situación*". Nuevamente, las cuestiones de atribución del hecho ilícito vuelven a tomar un protagonismo, por cuanto la intervención deliberada de agentes no estatales, que se hagan pasar por órganos del Estado, no podrá incurrir en dicha previsión. De nuevo la investigación forense será determinante para probar si, en efecto, es el Estado el que ha asumido el riesgo y si ese riesgo era o no inevitable. La actuación de terceros podrá conllevar la imposibilidad de que la actuación estatal sea fructífera a la hora de evitar la actuación ilícita. Sin embargo, no puede olvidarse el alcance de la obligación del Estado a la hora de impedir tales hechos, que ya ha sido expuesta al tratar la comisión del ilícito por omisión y sobre el que no procede ahora volver.

En siguiente lugar hay que hacer mención a los ciberataques que, producidos como consecuencia de una fuerza mayor, infrinjan una obligación internacional de DIH, que sea considerada imperativa, conforme a lo anteriormente expuesto. Como se viene exponiendo, en una situación de conflicto armado, a través de la actuación del Estado, será muy variada la casuística en relación a la infracción de obligaciones internacionales. El Estado, con carácter previo a la entrada en conflicto ha podido asumir frente a otros sujetos de Derecho Internacional, multitud de vínculos jurídicos cuyo mantenimiento se vea dificultado o impedido, precisamente por el conflicto bélico.

Sin embargo, las normas que son propias de dicho conflicto, habrán de ser observadas de modo tal que, en determinadas circunstancias y cuando la violación de la norma de DIH se produzca de forma grave y a gran escala, su incumplimiento, como se ha explicado, incurrirá en la violación de una norma imperativa. Por tal motivo, aun debiéndose a dicha causa de fuerza mayor, la violación de una norma imperativa de DIH a través de una ciberoperación, no encontrará ninguna justificación que excluya la responsabilidad internacional del

Estado. En este sentido, la exclusión que realiza el repetido artículo 26 del Proyecto resulta realmente evidente, pues de la literalidad de dicho texto no puede concluirse la presencia de ninguna excepción.

En consecuencia, cuando por una causa de fuerza mayor, se cometa cualquiera de los crímenes de guerra que se han expuesto anteriormente, como consecuencia de la violación de una norma de *ius cogens* de DIH, entrará en juego la aplicación de los artículos 40 y siguientes del Proyecto.

De tal manera, el Estado que se haya encontrado en la anterior circunstancia quedará obligado a "*cooperar para poner fin, por medios lícitos*" a dicha violación grave y, en modo alguno, podrá reconocer "*como lícita una situación creada por una violación grave en el sentido del artículo 40, ni prestará ayuda o asistencia para mantener esa situación* [805] ". Ello, "*sin perjuicio de las demás consecuencias enunciadas en esta parte y de toda otra consecuencia que una violación a la que se aplique el presente capítulo pueda generar según el derecho internacional*", es decir, de la sumisión de dicha conducta a la competencia de la Corte Penal internacional, en aplicación del artículo 8 de su repetido Estatuto.

3.4. El peligro extremo.

Asimismo, la ilicitud, a la luz del artículo 24 del Proyecto,

> "queda excluida si el autor de ese hecho no tiene razonablemente otro modo, en una situación de peligro extremo, de salvar su vida o la vida de otras personas confiadas a su cuidado".

Se trata, por lo tanto, de una situación en la que, la salvaguarda de determinados intereses, no permite otra decisión. En ese sentido, podría hablarse de otra modalidad de estado de necesidad, en tanto que la violación de la obligación internacional se comete con el único propósito de *salvar* la *vida,* sea propia o ajena. En relación con la fuerza mayor, la diferencia es radicalmente distinta pues aquí, en ningún momento, el Estado ha perdido el control de la situación.

805 Obligaciones, ambas, contenidas en el artículo 41 del Proyecto de artículos.

Antes bien, se trata de un hecho ilícito que se comete de modo intencionado y consciente, aun cuando la ilicitud quede posteriormente amparada por la salvaguarda de intereses superiores. Se tratará pues, de la violación de una obligación internacional que podría calificarse como inevitable. En este supuesto, la limitación es máxima, por cuanto, únicamente, la salvaguarda de la vida humana justifica la invocación de dicha causa, por lo que se tratará de una causa de justificación excepcional y, a su vez, comprobable *a posteriori*.

Al igual que en los supuestos anteriores, el Estado en conflicto, con el fin de salvaguardar vidas humanas, puede verse en la situación de incumplir una obligación internacional previamente contraída, sin que ello suponga una violación de las normas aplicables al combate, sino de cualquier otra de contenido diverso.

Como en los supuestos anteriores, queda impedida la aplicación de esta causa de justificación, en tasadas circunstancias. La primera de ellas es que la situación de peligro extremo se deba "*únicamente o en combinación con otros factores, al comportamiento del Estado que la invoca*". Es decir, en el ejemplo anterior, debería retomarse la argumentación ya expuesta en relación con la obligación del Estado de prestar seguridad. Sin embargo, no puede aquí trasladarse la responsabilidad del ataque al Estado que es atacado, pues, durante un conflicto armado, la aplicación del DIH impedirá el ataque a bienes y personas civiles. En consecuencia, para que esta causa de justificación no pudiera invocarse, la actuación del Estado que sufre el peligro debería haber sido flagrante, hasta el punto de haber omitido cualquier tipo se medida de seguridad informática en sus equipos militares o haber expuesto a sus combatientes al objetivo enemigo.

En cualquier caso, también aquí cobran importancia las cuestiones ya expuestas en relación con la atribución del hecho ilícito pues, en el momento en que dicho peligro se deba a la conducta del Estado, la violación de la obligación internacional será atribuible a dicho Estado y surgirá la responsabilidad internacional, sin que la acción u omisión pueda quedar amparada por dicha circunstancia.

En segundo lugar, tampoco será aplicable la exención de ilicitud con motivo de peligro extremo si "*es probable que el hecho en cuestión crea un peligro comparable o mayor*". Se trata ésta de una situación de mayor dificultad en cuanto a su constatación, por cuanto la comparación entre el peligro que se trata de evitar y el que se puede generar con la conducta ilícita conllevará siempre una valoración subjetiva.

Toda vez que el uso de internet pueda originar la consiguiente responsabilidad internacional, la introducción de este nuevo método de combate requiere, como en los aspectos que hasta ahora se han venido analizando, una nueva interpretación de determinados conceptos e incluso una nueva formulación de los mismos. En el aspecto que ahora se trata, no supone ello una novedad por cuanto, tradicionalmente, la práctica internacional, en relación al peligro extremo, había quedado limitada a supuestos muy limitados, siendo el Tribunal arbitral competente para conocer del caso *Rainbow Warrior* el que, al tratar el peligro extremo, como circunstancia de exclusión de la ilicitud, estableció una serie de requisitos, que bien podrían ser exigidos en otras circunstancias[806].

Así, en un conflicto armado en el que se lancen ciberoperaciones, hay que poner nuevamente de manifiesto el carácter imperativo de ciertas normas de DIH, respecto de las que ninguna justificación podrá invocarse tras su violación. Será, precisamente, en caso de conflicto armado donde la salvaguarda de vidas humanas, civiles y militares, se encuentre más amenazada. En este caso, la estricta aplicación de las normas del combate que se han ido exponiendo, será más que nunca necesaria para para lograr dicha salvaguarda, sin olvidar que el

806 Así lo pone de relieve el Comentario 9) al artículo 24 del Proyecto de artículos que aclara que, en este caso, "*El Tribunal aceptó por unanimidad que esa alegación era admisible en principio y por mayoría que era aplicable a los hechos en uno de los dos casos. En cuanto al principio, el Tribunal requirió a Francia que demostrara tres aspectos: 1. La existencia de circunstancias muy excepcionales de extrema urgencia que entrañen consideraciones médicas o de otro tipo de naturaleza elemental, siempre que posteriormente se obtenga de la otra parte interesada un reconocimiento rápido de la existencia de esas circunstancias excepcionales, o que se las pueda demostrar claramente; 2.El restablecimiento de la situación original de cumplimiento con la asignación en Hao no bien desaparezcan las razones de emergencia invocadas para justificar la repatriación; 3.La existencia de un esfuerzo de buena fe para tratar de obtener el consentimiento de Nueva Zelanda en los términos del acuerdo de 1986. Al igual que en el caso de fuerza mayor, una situación que ha sido causada o inducida por el Estado que invoca la excepción no es una situación de peligro extremo*".

DIH no prohíbe el uso letal de la fuerza. Antes bien, en aplicación del mismo, ese uso de la fuerza letal deberá acomodarse a las normas aquí estudiadas.

Habida cuenta que la salvaguarda de la vida e integridad física puede verse amenazada por los ataques informáticos, de igual modo que por un ataque realizado, empleando la fuerza cinética, la respuesta frente a este peligro extremo, podrá ofrecerse por métodos de combate convencionales o virtuales, pero en cualquier caso, con las limitaciones repetidamente expuestas. Si el Estado combatiente atacado inutilizara las redes informáticas del Estado atacante para frenar esa ciberoperación, vería su conducta incursa en la violación de la norma imperativa que exige la distinción entre objetivos civiles o militares, por más que invocara la presencia de un peligro extremo. En consecuencia, sería también aquí de aplicación el precepto que exige el cumplimiento de las normas infringidas. Es decir, el Estado agresor debería cesar ese ciberataque contra la red informática y el agredido debería detener su respuesta, tan pronto fuera posible. Si además, aludiendo a un peligro extremo, dicha violación se cometiera de forma grave y a gran escala, se estaría contraviniendo una norma imperativa, lo que impediría cualquier justificación del ilícito.

3.5. El estado de necesidad.

Por último, con carácter previo a examinar la legítima defensa, se hará mención a la siguiente de las causas de justificación del hecho ilícito prevista por el Proyecto.

De modo similar a la previsión que se contiene en el Derecho interno, el artículo 25 del Proyecto entiende que

> "1. Ningún Estado puede invocar el estado de necesidad como causa de exclusión de la ilicitud de un hecho que no esté de conformidad con una obligación internacional de ese Estado a menos que ese hecho:
>
> a) Sea el único modo para el Estado de salvaguardar un interés esencial contra un peligro grave a inminente; y
>
> b) No afecte gravemente a un interés esencial del Estado o de los Estados con relación a los cuales existe la obligación, o de la comunidad internacional en su conjunto.

2. En todo caso, ningún Estado puede invocar el estado de necesidad como causa de exclusión de la ilicitud si:

a) La obligación internacional de que se trate excluye la posibilidad de invocar el estado de necesidad; o

b) El Estado ha contribuido a que se produzca el estado de necesidad".

En este caso, la diferencia con la causa de justificación consistente en el peligro extremo radica, como se pone de manifiesto en el Comentario al Proyecto, no ya en la vida de las personas que ha de ser salvaguardada por el Estado, sino en el interés del propio Estado o de la Comunidad Internacional, en su conjunto[807].

De igual modo que en las causas hasta ahora vistas, nos encontramos ante una circunstancia cuya excepcionalidad es evidente, tal y como la Jurisprudencia internacional ha puesto de relieve. En este sentido, la CIJ ha justificado, incluso, que la redacción dada a este artículo 25 por el Proyecto, lo sea en forma negativa[808]. En efecto, de esta manera, la prohibición del hecho ilícito se muestra más clara y, únicamente, cuando concurren las dos circunstancias arriba recogidas, puede entenderse que existe un estado de necesidad. Por ese mismo motivo, se considera que ambas circunstancias han de darse de forma conjunta y no disyuntiva[809].

El concepto de estado de necesidad, propio del ámbito penal se recoge en el Derecho interno de forma, aparentemente, más detallada, por cuanto la

807 Así se afirma en el Comentario 1) al artículo 25 del Proyecto, cuando se define el estado de necesidad como "*la única forma que tiene un Estado de salvaguardar un interés esencial amenazado por un peligro grave e inminente*", de forma que el mismo queda a salvo cuando se opta por "*no cumplir otra obligación internacional de menor importancia o urgencia*".

808 En este sentido, la CIJ en el asunto Proyecto Gabcíkovo-Nagymaros estableció que "*The International Law Commission was of the same opinion when it explained that it had opted for a negative form of words in Article 33 of its Draft*". GabCikovo-Nagymaros Project (HungarylSlovakia), Judgment, I. C. J. Reports 1997; par. 51.

809 "*Thus, according to the Commission, the state of necessity can only be invoked under certain strictly defined conditions which must be cumulatively satisfied; and the State concerned is not the sole judge of whether those conditions have been met*". GabCikovo-Nagymaros Project (Hungary/Slovakia), Judgment, I. C. J. Reports 1997; p. 51.

justificación, prevista en el apartado 5 del artículo 20 del Código Penal exige la proporcionalidad en la reacción, la falta de provocación del estado de necesidad y ausencia de obligación profesional. Sin embargo, el Proyecto exige, al sujeto de Derecho Internacional que pretenda la aplicación de esta causa, una mayor labor de interpretación. Así, qué haya de entenderse por "*interés esencial*" o en qué momento un peligro resulta "*inminente*" y de "*gravedad*" suficiente, quedará a juicio del Estado que lo invoque. En este punto, habrá que tener presentes las causas anteriormente examinadas, de forma tal que, un interés esencial deberá ser distinto del supuesto que quede amparado por las situaciones de fuerza mayor y peligro extremo.

La excepcionalidad que se predica se pone, aun más, en evidencia, al establecer el segundo párrafo del artículo 25 que, además, será inoperante dicha causa de justificación cuando "*la obligación internacional de que se trate excluye la posibilidad de invocar el estado de necesidad*" o si el referido Estado hubiera "*contribuido a que se produzca el estado de necesidad*".

Nuevamente, la primera de las excepciones no plantea ninguna duda, pues no pretende sino salvaguardar la legalidad internacional. En el segundo de los supuestos, también, nos encontramos ante la imposibilidad de invocar la causa en aquellos casos en que la intervención del Estado haya sido determinante para la producción del estado de necesidad. De forma coherente, el Proyecto desarticula la posibilidad de que el comportamiento inadecuado en el ámbito internacional pueda favorecer a quien lo realiza. De igual modo serán aquí de aplicación las consideraciones precedentes relativas a las cuestiones de atribución y de las obligaciones relativas al Estado que, por haber sido repetidamente expuestas, no van a analizarse de nuevo.

Por último, resulta relevante a la cuestión que aquí se trata, el hecho de que la causa de justificación no opere en cuanto el ilícito, cometido a través de su ejercicio, "afecte gravemente a un interés esencial del Estado o de los Estados con relación a los cuales existe la obligación, o de la *comunidad internacional en su conjunto*". Del texto parece deducirse que se trata de preservar intereses superiores a los del Estado, en relación con otros Estados. Sin embargo, en lo que

respecta a las obligaciones que dicho Estado tenga con la Comunidad Internacional en su conjunto, nos encontraremos ante las normas de *ius cogens* o imperativas que caerán, nuevamente, dentro de la específica regulación que para ellas prevén los artículos 26 y 40 y siguientes del Proyecto, ya vistas.

4. CONCLUSIÓN AL CAPÍTULO QUINTO.

El ciberataque utilizado como método de combate constituye un hecho ilícito cuando el mismo viola una norma de DIH, en el sentido expuestso a lo largo del presente trabajo. Pues bien, sin omitir la aplicabilidad del resto de causas o circunstancias de exclusión de la ilicitud, el ámbito bélico en el que este hecho ilícito va a desarrollarse confiere una especial importancia a la legítima defensa, respecto de la que puede ofrecerse la siguiente conclusión:

ÚNICA: La legítima defensa no justificará la utilización de un ciberataque prohibido por el DIH. En el ámbito de los ciberataques utilizados, durante el conflicto armado, como método de combate, se producirá la justificación del ilícito cuando la legítima defensa cumpla con los requisitos que se contienen en la Carta de Naciones Unidas. Si un ciberataque puede constituir un ataque armado, la legítima defensa frente al mismo ha de estar prevista como una respuesta coherente con la agresión. Sin embargo, la defensa ejercida a través de un ciberataque contario al DIH nunca podrá justificar tal reacción.

En relación a la primera cuestión, también la legítima defensa presenta una serie de particularidades, cuando en el desarrollo del combate sea ejercida a través de métodos cibernéticos. La existencia de la agresión es el primero de los requisitos de legitimidad de la acción defensiva y, para ello, hay que volver a traer a colación el concepto restrictivo de ciberataque armado que se defiende a lo largo de todo el presente trabajo. Únicamente cuando el ciberataque que se reciba pueda considerarse un ataque armado, habrá ocasión de invocar, frente al mismo, la legítima defensa. No cabe, pues, aceptar la reacción defensiva frente a ciberactividades que no revisten la gravedad del ataque armado. Vuelven aquí a cobrar importancia la delimitación conceptual que se realizaba en el Primer

Capítulo y la distinción del ciberataque armado respecto de otras manifestaciones en la red, que se trataban en el segundo, pues de otra manera podría incurrirse en el error de aceptar una respuesta en legítima defensa, en el combate, frente a actuaciones inofensivas o que quedan fuera del DIH.

En virtud de lo anterior, convendría que, por parte del Consejo de Seguridad de Naciones Unidas, se autorizara el ejercicio de la legítima defensa, únicamente, frente a este tipo de ataques. Esta tesis restrictiva favorecerá el respeto a la legalidad internacional e incrementará la seguridad jurídica, al menos, en tanto que dicha legalidad internacional no prevea un concepto expreso de ciberataque armado ni exista la suficiente práctica estatal. En caso contrario, parece evidente y previsible un aumento de la conflictividad internacional y un uso de la fuerza desmesurado, pues la actividad en internet ha presentado, hasta ahora, unos signos de violencia y habitualidad que, si son objeto de una calificación jurídica incorrecta, pueden originar reacciones defensivas ilegítimas. Esta actuación por parte del Consejo de seguridad de las Naciones Unidas, por otra parte, resultará determinante, cuando la legítima defensa vaya a ser ejercida por la OTAN y, también, por la UE, cuando se trate de activar la cláusula de asistencia mutua, prevista en el TUE. Dado que tanto la OTAN como la UE han de someter su actuación a la legalidad emanada por las Naciones Unidas, debería ser ésta última Organización la que impusiera un criterio estricto, que evitara el aumento de la beligerancia.

Por otra parte, pero con base en los mismos argumentos, la legítima defensa frente a un ciberataque armado deberá ser siempre coetánea al mismo, debiendo abandonarse las tesis que defienden la posibilidad de defensa frente a actos hostiles que no se han producido. La respuesta en legítima defensa que no sea coetánea con el ciberataque que se recibe, tendrá que ser calificada jurídicamente como una represalia o bien un ataque en sí mismo, pero en modo alguno una defensa legítima.

Por último, la defensa deberá ser proporcional a la agresión sufrida, sin que se aprecie tampoco impedimento para que este requisito sea exigido cuando, en el desarrollo de un conflicto armado, se empleen métodos de combate

virtuales. Esta proporcionalidad, no obstante, no exige una identidad de métodos de combate y así, frente a un ciberataque podrá responderse a través de métodos de combate convencionales y viceversa. La proporcionalidad se guardará en función de la gravedad y modalidad de la agresión y de la propia necesidad del uso de la fuerza.

En conclusión, la respuesta ante ciberataques que no constituyan una agresión cometida a través de este método de combate impedirá la respuesta en legítima defensa. Asimismo, será contraria a la legalidad internacional la defensa que se realice frente a un Estado al que no se puede atribuir el ciberataque, en los términos que se veían en el Capítulo precedente, donde se puso de manifiesto la dificultad e incluso imposibilidad de atribución al Estado de los ciberataques cometidos por agentes no estatales.

En consecuencia, la inobservancia de los requisitos anteriores implicará la violación de una obligación internacional por parte del Estado que ejerce su defensa. Si a través de dicha reacción defensiva se cometiera un hecho ilícito contrario al DIH, además, nos encontraremos ante la violación de una norma imperativa. Esta contravención se producirá cuando, en el desarrollo del conflicto, se ejerza la defensa a través de un ciberataque utilizado como método de combate prohibido. Por lo tanto, la reacción defensiva que carezca de necesidad militar será contraria a la norma de *ius cogens* que se analizaba en el capítulo segundo y no permitirá justificar el hecho ilícito, en virtud de una legítima defensa. De igual modo hay que concluir en relación con la defensa del Estado que se cometa a través de un ciberataque dirigido a objetivos civiles o que cause un daño innecesario o desproporcionado. Nada permitirá, en estos casos, amparar la conducta del Estado en la legítima defensa, pues no concurrirá dicha legitimidad. De igual manera ocurrirá si la defensa del Estado se realiza a través de un ciberataque que provoque un engaño tal que sea considerado pérfido o violando el respeto a la neutralidad de terceros.

CONCLUSIONES FINALES

La investigación que ha sido abordada permite concluir que la singularidad de los ciberataques y, por lo tanto, la incorporación a los conflictos armados de un método de combate virtual incide, directamente, en los conceptos que configuran la responsabilidad internacional del Estado.

Cuando en el desarrollo de los conflictos armados, los Estados se valgan de armas cibernéticas y éstas se utilicen violando alguna de las obligaciones de DIH, de entre las consideradas inconculcables, podrá exigirse al Estado infractor la correspondiente responsabilidad internacional. Sin embargo, con carácter previo a dicha exigencia habrá que tener en cuenta que este método de combate implica una nueva interpretación de las cuestiones clásicas relativas a la responsabilidad internacional del Estado, que llevan a las siguientes conclusiones,

I

La legalidad internacional solo podrá garantizarse partiendo de un concepto restrictivo de ciberataque, aplicable al conflicto armado internacional y no internacional.

La aparición de los ciberataques supone la introducción de un fenómeno tan novedoso como determinante en el desarrollo de los conflictos armados modernos, que requiere una calificación jurídica apropiada, al igual que el resto de actuaciones que pueden darse en el combate.

Los nuevos métodos de combate han supuesto una distorsión en el desarrollo de los conflictos armados que, actualmente, permite hablar de conflictos asimétricos[810] e híbridos[811]. Estas tipologías de conflictos ya se daban con carácter previo a la aparición de los ciberataques. Tanto un tipo de conflicto

[810] GEISS, R. Las estructuras de los conflictos asimétricos, op. cit., pp. 1-23.
[811] En relación a este concepto, nos remitimos, nuevamente, al estudio del mismo realizado por SÁNCHEZ HERRÁEZ, P. *La nueva guerra híbrida: un somero análisis estratégico*, doc. cit.

como otro, se han producido con carácter previo a la aparición de los ciberataques y, de hecho, podrían seguir produciéndose sin ellos, pero parece evidente que la irrupción de este tipo de ataques introduce un factor adicional en el incremento del carácter híbrido y de la asimetría del conflicto bélico.

En ambos casos, a los factores, aparentemente, ajenos al combate se une un elemento novedoso, respecto del que no existe una regulación internacional que lo recoja expresamente. Además, en el caso de los ciberataques se da la circunstancia de que nos encontramos ante un elemento que admite una alta disponibilidad por parte de la población civil. En consecuencia, cuando el ciberataque es utilizado en un conflicto armado, incrementa la inseguridad jurídica, en relación a la calificación de los hechos cometidos y la atribución de su autoría. Esta incertidumbre, nuevamente, no es propia, exclusivamente, de los ciberataques, pues ya se había constatado al pretender establecer un régimen jurídico inequívoco para los terroristas en combate. En principio, la aplicación del DIH a los autores de actos terroristas, durante el combate, no parece una solución que pueda adoptarse sin discusión, sino, antes bien, una respuesta que tendrá que evitarse en la mayor parte de las ocasiones. Sin embargo, en este caso, que pudiera parece el de mayor similitud con los ciberatacantes, la laguna jurídica que se aprecia es relativa, pues existe una legalidad interna e internacional, aplicable al terrorismo, en defecto y, en ocasiones, con carácter prioritario al DIH.

Por lo tanto, la situación que presentan los ciberataques cuando son empleados en el combate, resulta ciertamente novedosa, pues, en principio, el vacío legal respecto de los mismos es completo.

Por este motivo, el consenso que se alcance en relación al concepto de ciberataque es primordial y no permite admitir una definición que no resulte acorde con la legalidad internacional. Tampoco puede admitirse un vacío de legalidad, motivado por la ausencia de una regulación expresa. Antes bien, el concepto de uso y amenaza del uso de la fuerza presente en la Carta de Naciones Unidas y en las Resoluciones del Consejo de Seguridad de la misma Organización, tiene que ser aplicado a esta nueva modalidad de ataque. Puesto que dicha aplicación, ineludiblemente, ha de realizarse a través del método

analógico, se trata de una labor que requiere la aplicación restrictiva de los criterios que en ella se tengan en cuenta.

Es preciso por consiguiente, descartar cualquier propuesta que suponga una ampliación injustificada del concepto de ataque armado y, que, por lo tanto, se aparte del concepto de uso o amenaza de la fuerza, tal y como se recoge por los instrumentos citados de las Naciones Unidas.

La participación de agentes no estatales en estos conflictos, además, aconseja la adopción de un criterio restrictivo. La accesibilidad a internet de gran parte de la población, en los conflictos que se libran en gran parte de los Estados, impone una conceptuación que impida considerar que otras conductas que, en realidad, no pasarán de ser ciberincidentes o ciberdelitos sean un ataque armado. La restricción conceptual presenta indudables ventajas en relación a los conflictos armados internacionales, pues de este modo se conseguirá una limitación en el uso de la fuerza y también ayudará a reducir la beligerancia en la escena internacional. Pero, en este sentido, tampoco puede desatenderse la influencia positiva que tendrá en los conflictos armados no internacionales. La adopción de un concepto amplio, por el contrario, tendría como consecuencia la calificación jurídica de conflicto armado no internacional de situaciones que no pasan de ser disturbios internos, aun cuando los mismos, al desarrollarse a través de la red, resulten especialmente virulentos. En el caso de que no se limitara esta calificación de ciberataque armado a aquéllos que realmente constituyan un ataque, podría darse la situación de que la actuación del Estado incidiera directamente en traspasar el umbral de la violencia requerido para la constatación de un conflicto armado no internacional, con las indeseables consecuencias que ello podría tener.

Además, esta restrictividad viene, además, impuesta por la consideración de internet como arma de doble uso. Esta condición se vislumbra claramente en el uso que pueden realizar de internet los individuos, pero también ha de ser tenida en cuenta al valorar la actuación de uno de los principales agentes estatales: las Fuerzas Armadas. Esta naturaleza de arma de uso dual se pondrá de manifiesto, constantemente en el desarrollo del combate, de manera que los

mismos verán conducidas sus comunicaciones a través de la red de manera habitual. Por este motivo, pues, es también necesario que el concepto de ciberataque armado quede limitado a aquéllos supuestos en que a través de internet se lance realmente un ataque y no se aplique a los incidentes que pudieran ocurrir en las redes militares, durante el conflicto.

Por otra parte, esta condición de arma de doble uso, impone, asimismo, la aplicación del DIH a los ciberataques que tengan la naturaleza de como método de combate y, por ende, deberá limitarse a los que reunan dichas condiciones y no a cualquier uso malicioso de la red.

Por último, en la adopción del concepto de ciberataque armado, se impone una actuación preeminente del Consejo de Seguridad de las Naciones Unidas, a través de la calificación jurídica que, en cada caso, otorgue a ciberincidentes que susciten dudas en cuanto a su naturaleza jurídica. La preeminencia de la Organización deberá quedar de manifiesto, habida cuenta la función de garante de la "paz y la seguridad internacionales[812]", que le corresponde en el contexto internacional. Por otra parte, la previsible utilización de los ciberataques como métodos de combate en los futuros conflictos armados, por parte de la OTAN y la UE, deberá basarse en un concepto de ciberataque armado que esté delimitado por las Naciones Unidas y cuya definición no ofrezca dudas ni deje a los Estados la posibilidad de una interpretación ampliatoria.

II

Un ciberataque contrario a las normas de DIH es un método de combate prohibido.

La consecuencia lógica de la consideración de internet como método de combate consistirá en la aplicación, al mismo, de las normas de DIH que rigen el uso de todo método de combate que se utilice en un conflicto armado. La

[812] Artículo 1 de la Carta de Naciones Unidas.

aparente laguna jurídica, pues, que se advierte *a priori,* en relación a los ciberataques armados, no puede admitirse.

La aplicación de los principios inconculcables que se establecen por la CIJ en su Opinión Consultiva en relación con la legalidad de las armas nucleares, configura un régimen jurídico del que no pueden sustraerse los ataques armados cometidos por internet.

En consecuencia, la licitud del método de combate dependerá directamente del cumplimiento de las limitaciones que imponen las normas de DIH y, por lo tanto, será necesario interpretar las mismas, de forma tal que el elemento cibernético tenga cabida.

En esta tarea, no se puede partir de una mera traslación de términos, sino que, en el diseño de cada ciberoperación, el Mando militar encargado de ello tendrá que tener presentes las peculiaridades del elemento cibernético. El diseño de las operaciones militares que, posteriormente, tenga su reflejo en el Plan de Operaciones y su Anexo de ROE´s deberá valorar todas las limitaciones que al cibercombate impone el DIH y, por lo tanto, evitar cualquier ataque informático que no se corresponda con una necesidad militar. La posibilidad real de producir un ataque, a través de la red, revelará, en ciertos casos, una superioridad militar que hay que valorar mesuradamente. El hecho de que, materialmente, un ataque sea posible, no puede suponer un uso del mismo que no se corresponda con un objetivo militar. Incluso en aquéllos casos en que el daño no fuera grave o desproprocionado no podrá admitirse un ciberataque que no responda a esa necesidad y que se lance a modo de ejercicio o incluso de forma experimental.

Asimismo, la obligación de distinguir entre objetivos civiles y militares conllevará una labor adicional, si tenemos en cuenta el carácter de uso dual de internet que se ha mencionado y la interconectividad de redes. Nuevamente aquí, se defiende una valoración minuciosa de los objetivos y de los efectos del ataque. Precisamente esta dificultad de distinción tiene que corresponderse con un mayor rigor en el diseño y lanzamiento del ciberataque y no puede tomarse como justificación de un ataque a objetivos civiles, sean éstos personales o materiales. Los bienes jurídicos que pueden resultar lesionados con un ciberataque son de la

misma entidad que los que se lesionan a través de métodos de combate tradicionales y, por ese motivo, la obligación de distinguir no puede infravalorar los efectos del ciberataque.

Por la misma causa, el ciberataque que cause daños desproporcionados o innecesarios tiene que evitarse, pues, de otro modo, el uso de este método de combate estará prohibido. La evitación de esos daños desproporcionados o innecesarios requiere una estimación de los mismos, antes de lanzar cualquier ataque y, en este caso, tendrá que tener en cuenta, por ejemplo, la sencilla propagación de los virus informáticos insertos, en correos electrónicos. La posibilidad de que dichos correos sean difundidos, a su vez, por los destinatarios que ignoran sus efectos, es realmente alta, sobre todo si estos destinatarios carecen de la adecuada formación en ciberseguridad. Esta situación parece probable si, por ejemplo, se difundiera un correo malicioso entre el personal de un Contingente en combate, que simulara proceder de una Organización Internacional. Con seguridad, los efectos que el mismo produjera podrían incurrir en desproporción o innecesariedad.

Asimismo, esa posibilidad de enmascarar la identidad del remitente puede utilizarse para el lanzamiento de un ciberataque que incurra en perfidia. Por este motivo, hay que reiterar la necesidad de que el diseño y lanzamiento de las ciberoperaciones no se realicen al margen de su adecuación al DIH. El envío de un correo de las características antes dichas, podría darse simulando, por el remitente, gozar del estatuto de persona civil, no combatiente, o de un estatuto de protección. Si con ese correo se pretendiera matar, herir o capturar a un adversario, el método de combate cibernético deberá ser descartado, por estar prohibido por el DIH, al incurrir en perfidia. Si un hospital de campaña abriera un correo con apariencia de provenir de la Cruz Roja Internacional o de Naciones Unidas y, a través del mismo, quedara comprometida la operatividad de su red, no parece difícil que se consiguieran los resultados enunciados y que se recogen en el PA I.

Por último, el planeamiento de una ciberoperación no podrá valerse de redes de Estados que se hayan declarado neutrales. Nuevamente, las capacidades

militares para realizar una intrusión en servidores o cualquier otro tipo de ciberinfraestructura de otro Estado tendrán que ponerse en relación con las limitaciones que en este aspecto impone el DIH.

En todos los casos, pues, se impone una valoración realista de las capacidades y efectos de los ciberataques en el combate que comiencen por la consideración restrictiva del concepto de ciberataque. Una vez delimitado el mismo, no puede confundirse la capacidad, desde un punto de vista práctico de diseñar y planear una ciberoperación, con la legitimidad de la misma, pues la novedad del elemento cibernético y su ausencia de regulación expresa podrían dar lugar a decisiones erróneas.

III

Las medidas de reparación no pueden obviarse por el hecho de que la violación de la obligación se haya producido de forma virtual.

Sin embargo, esta modalidad comisiva del hecho ilícito tiene una incidencia directa en el modo en que dichas medidas van a ser aplicadas.

La primera de las obligaciones a las que debe atender el Estado infractor consiste en la cesación de la violación de la obligación. Pues bien, el cumplimiento de esa primera y elemental obligación se verá limitado cuando los ciberataques se lancen como método de combate prohibido por el DIH. En el caso de que se viole una obligación de DIH, a través de un método de combate convencional, será habitual que dicha violación se manifieste de forma clara y, en muchas ocasiones, de modo inmediato. Sin embargo, en el caso de los ciberataques no será lo habitual. La utilización de un arma virtual ofrece la ventaja de que puede hacer surtir sus efectos durante un largo lapso de tiempo sin mostrar su presencia. En consecuencia, este método de combate impedirá la cesación inmediata de la violación, pues aunque se imponga la misma inmediatamente después de conocerse el ataque, rara vez podrá imponerse al comienzo de la violación.

No puede afirmarse que esta singularidad venga exclusivamente referida a los ataques virtuales, pues las tácticas de combate, a través de métodos convencionales contemplarán, asimismo, el ocultamiento al enemigo. Sin embargo, en este caso, más que en otros hay que tener presente que esa facilidad de ocultación constituye una ventaja adicional para las Fuerzas Armadas en combate, que puede hacer preferible el ciberataque frente a otros métodos. En consecuencia, cuando por medio de un ciberataque se viole una norma de DIH, la primera obligación atinente al Estado infractor podrá verse limitada en su cumplimiento.

De idéntico modo, la obligación de cumplir con la obligación que ha sido violada podrá verse afectada cuando el ciberataque siga produciendo efectos, fuera del control del Estado responsable de su lanzamiento. La necesidad de acatar inmediatamente la obligación incumplida podrá verse impedida si, por ejemplo, se ha introducido un virus informático que sigue propagándose entre usuarios civiles, sin que éstos conozcan el modo de detenerlo o no tengan capacidad para hacerlo.

Cuando el mecanismo de reparación entre en funcionamiento, la restitución será la siguiente medida que deberá aplicarse. Nuevamente, el hecho de que un ataque armado sea lanzado por un medio virtual añadirá una dificultad a la obligación de reparar, pues la acreditación del daño, efectivamente producido, se verá severamente condicionada. Una evaluación exacta, por parte del Estado que haya sufrido el ciberataque, equivaldrá, en ocasiones, a desvelar los fallos que ese Estado ha encontrado en su ciberseguridad. Si, en cualquier combate, las vulnerabilidades militares han de ocultarse al enemigo, en este caso, las fisuras en las medidas de seguridad cibernéticas resultan una debilidad mayor, pues podrían ser aprovechadas incluso por terceros ajenos al combate. Todavía con mayor razón será difícil que se revelen los daños producidos si la ciberseguridad depende, en algún extremo, de una compañía privada que preste servicios al Estado, pues las futuras repercusiones para la misma son evidentes. Asimismo, la indemnización económica del daño causado al Estado lesionado, podría encontrar similares dificultades.

Por último, entrarán en juego las medidas destinadas a proporcionar una satisfacción al Estado lesionado. Al igual que en los casos anteriores, la aplicación del Proyecto de artículos no podrá cuestionarse, pero sí que se verá condicionada por el hecho de que la violación de la obligación internacional sea cometida virtualmente. En este supuesto, destinado, principalmente, a la satisfacción moral por el descrédito o el deshonor causados al Estado lesionado, la reparación también se halla condicionada. Si el Estado infractor opta por presentar disculpas o por el reconocimiento de la autoría del hecho ilícito, deberá tener presente la repercusión que su hecho haya alcanzado en la red y la dispersión de sus efectos.

Por este motivo, además, será preciso que quienes sean responsables del planeamiento de las Operaciones cibernéticas sean conscientes de la ulterior responsabilidad en que puede incurrir el Estado, como consecuencia de la utilización de un ciberataque contrario al DIH. La formación y adiestramiento en DIH, necesaria y obligatoria para los miembros de las Fuerzas Armadas, deberá contener, pues, la consiguiente mención a la responsabilidad en que incurrirá el Estado por la contravención del DIH y a las medidas reparadoras a que queda obligado.

La posibilidad de diseñar operaciones cibernéticas en las que el objetivo final siempre será un equipo informático y no un individuo puede motivar que quien planea la ciberoperación, experimente un distanciamiento inicial, respecto de las repercusiones finales del ciberataque que, en todo caso, hay que evitar. La formación en materia de DIH es más necesaria, en este ámbito, que en el empleo de otros métodos de combate en los que el resultado se produce directamente en un objetivo personal o material y ese resultado está previsto desde el inicio del planeamiento. En esta labor de formación no puede olvidarse la última de las consecuencias que esa ciberoperación puede tener, que es la exigencia de responsabilidad del Estado infractor, a través de la obligación de reparar.

IV

El cumplimiento de la legalidad internacional impedirá, en números casos, atribuir al Estado un ciberataque prohibido por el DIH, que se utilice como método de combate, por agentes no estatales.

El criterio restrictivo que se propone en la delimitación conceptual de los ciberataques armados, ha de seguir manteniéndose en materia de atribución al Estado de los hechos ilícitos cometidos cuando aquéllos se utilicen como método de combate. Si la responsabilidad del Estado parece evidente cuando se trata de responder de ciberataques cometidos por sus Fuerzas Armadas, contraviniendo el DIH, la participación de agentes no estatales en el conflicto, dirige a la conclusión contraria.

Como se ha expuesto, la disponibilidad de este método de combate por agentes no estatales implica una nueva configuración de los conflictos armados. El conflicto de carácter híbrido y la asimetría tendrán lugar, con mayor facilidad, al entrar en combate agentes no estatales que dispongan de este método.

Sin embargo, tampoco aquí puede abogarse por un criterio de atribución al Estado de tal amplitud que contravenga la legalidad internacional. En efecto, se trata de un fenómeno al que habrá que dar respuesta, pues, de lo contrario, la incentivación por parte de los Estados, para que los individuos o grupos de cibervoluntarios, se involucren en el conflicto armado, lanzando ciberataques, incrementaría esa asimetría que se cita. Las posibilidades de actuar en redes ocultas o con mayor facilidad para ocultar la identidad que con otros métodos de combate, puede incentivar que, incluso los Estados se valgan de una actividad realizada por personal ajeno a sus Fuerzas Armadas. No obstante, esto no puede justificar que se defiendan criterios ajenos a la legalidad en materia de atribución al Estado. Las razones que se exponían al defender un criterio restrictivo de ciberataque vuelven a cobrar vigencia, pues tanto en los conflictos armados internacionales como no internacionales, la atribución al estado de hechos ilícitos cometidos por individuos podría ocasionar un aumento de la beligerancia.

Asimismo, no sería descartable una aplicación inadecuada del DIH, en tales supuestos.

Por el contrario, cuando se desarrollen actividades en la red, por agentes no estatales, durante el conflicto armado, habrá que tener muy presente el concepto de ciberataque armado. La realización de actividades reivindicativas, de apoyo a una de las partes en combate e incluso de enaltecimiento de la violencia, se darán, a buen seguro, en la red mientras persista el conflicto, pero no podrán calificarse de ataque armado cibernético. Cuando esta calificación jurídica sea posible, el criterio de atribución al Estado deberá reunir los requisitos para considerar que ese personal civil participa directamente en las hostilidades.

La defensa de un control estricto por parte del Estado resulta ineludible, sin que pueda considerarse una teoría superada por las que abogan por un control general. La aparente dicotomía manifestada, entre ambas posiciones jurisprudenciales, principalmente en los pronunciamientos de la CIJ, en la Sentencia relativa las Actividades Militares y Paramilitares en y contra Nicaragua, y del TPAY, en su Sentencia del caso Tadic, ha de resolverse, en este caso, a favor de la primera. No se trata, a nuestro juicio, de dos posiciones completamente encontradas, sino de una evolución en la teoría del control del Estado que, finalmente, admite un examen de las circunstancias, caso por caso. Por lo tanto, asumiendo este postulado, nos encontramos con que, la participación de los cibervoluntarios en el conflicto exigirá que, por parte del Estado en cuyo favor combatan, se pruebe un control estricto de sus actuaciones. Los argumentos que pudieran llevar, *a priori*, a defender un control global tienen que ser descartados, en favor del que aquí se defiende. El hecho de que esta participación se vaya a presentar con relativa frecuencia y, hasta con facilidad, para estos cibervoluntarios y la dificultad en la prueba del nexo con la actuación del Estado, deben conducir a sostener la necesidad de apreciar un control estricto del Estado. En caso contrario, como ocurriría si se adoptara un criterio laxo para la definición de ciberataque armado, la conflictividad entre Estados se vería incrementada. Si la atribución de los ciberataques armados de los cibervoluntarios no respondiera a este control, el recurso a la legítima defensa por parte del Estado agredido se

estaría autorizando de forma desmedida, favoreciendo, como se ha apuntado, un incremento de las hostilidades.

Por otra parte, tampoco se aprecian las ventajas de admitir ese control general en los supuestos en que las actividades se produjeran en el contexto de un conflicto armado no internacional pues podría originar, asimismo, un aumento de la violencia interna. Por último, tampoco puede aquí olvidarse la posibilidad, otras veces señalada, de que quien comete un ciberataque simule una identidad falsa. A través de esta técnica, podrían atribuirse al Estado ciberataques que, en realidad, no han sido cometidos por éste y que son lanzados por cibervoluntarios con la intención de involucrar a un Estado en un conflicto armado internacional o no internacional. En consecuencia, la necesidad de que el control del Estado sobre los participantes civiles en las hostilidades sea estricto, resulta insoslayable.

V

Atendiendo a los caracteres y criterios de identificación del *ius cogens*, la utilización de un ciberataque como método de combate prohibido por el DIH puede constituir la violación de una norma imperativa y, en consecuencia, un ciberataque prohibido por el DIH no justificará el hecho ilícito cometido.

A la luz de la definición ofrecida por el artículo 53 de la Convención de Viena sobre los Tratados, se ha podido constar que las normas prohibitivas de DIH en relación con los métodos de combate, aplicables a los ciberataques pueden ser consideras normas universales, imperativas y protectoras de bienes jurídicos superiores. Además, se entenderá que estamos ante una violación grave, atendiendo al Proyecto de artículos sobre responsabilidad internacional de los Estados por hechos internacionalmente ilícitos, cuando se produzca la violación flagrante y sistemática de una norma de DIH. Por lo tanto, la utilización de un ciberataque, como método de combate que incurra en tales condiciones, se tendrá por la violación grave de una norma imperativa.

Desde el momento en que sea lanzado un ciberataque, violando de forma flrgante y sistemáticas las normas prohibitivas de DIH en relación con los métodos de combate, no sería posible justificar la comisión de dicho hecho ilícito, amparándose en cualquiera de las circunstancias o causas de exclusión de la ilicitud. Al contrario, sería de aplicación el artículo 26 del Proyecto de artículos sobre responsabilidad internacional de los Estados por comisión de hechos ilícitos.

VI

El ciberataque que viole de forma grave las normas de DIH será un crimen de guerra y no quedará amparado por la legítima defensa.

La consideración de las normas imperativas, en relación a las limitaciones de DIH aplicables al combate, tiene como primera consecuencia la posibilidad de que, a través de un ciberataque armado, pueda cometerse un crimen de guerra. A lo largo del presente trabajo se han expuesto las posibilidades de que ofrecen los ciberataques, desde un punto de vista práctico, a la hora de producir los resultados que, hasta el momento, se conseguían a través de métodos de combate convencionales. Por lo tanto, hay que concluir que a través de los ciberataques podrán cometerse los crímenes de guerra que se prevén en el Estatuto de la CPI.

Sin embargo, tampoco aquí cabe una mera traslación, a las ciberoperaciones, de la doctrina general aplicable al resto de métodos de combate. Antes bien, las dificultades que presenta el uso de internet como método de combate se pondrán de manifiesto, nuevamente y, si cabe, con mayor intensidad.

Una de las consecuencias de la anterior conclusión será que la comisión de crímenes de guerra, a través de ciberataques armados prohibidos por el DIH, durante el conflicto armado, impide que el hecho ilícito quede amparado por las causas de justificación contenidas en los artículos 20 y siguientes del Proyecto. De entre las previstas en dichos artículos, cobra especial relevancia la legítima defensa, por cuanto, en el ámbito del conflicto armado, será la que, con toda seguridad, se invoque con mayor frecuencia. Asimismo, los conflictos bélicos más

recientes, demuestran cómo, precisamente es la legítima defensa la cuestión jurídica que suscita mayor controversia[813].

Cuando en el desarrollo del combate, las Fuerzas Armadas de un Estado reciban un ciberataque armado, la posibilidad de repeler la agresión en legítima defensa queda, evidentemente, limitada por el cumplimiento del DIH. Pero, además, a la hora de constatar la existencia de los requisitos exigibles a la actuación en legítima defensa, serán de aplicación las consideraciones realizadas a lo largo de este trabajo.

Es decir, en primer término, será preciso que dicha defensa se realice respeto de un ciberataque armado y no de una actividad cibernética que no revista tal carácter. El concepto estricto de ciberataque que se defiende cobra aquí una nueva dimensión, en tanto que, si la respuesta se ejerce respecto de un ciberataque que no constituya ataque armado, podría considerarse carente de necesidad militar o desproporcionada. En consecuencia, el Estado que, a través de sus Fuerzas Armadas, respondiera de ese modo, incurrirá en una violación de DIH, que, en caso de ser grave, constituirá un crimen de guerra.

En segundo lugar, cuando, en efecto, el ciberataque pudiera considerarse un ataque armado, la atribución al Estado debe realizarse sin que quepa ninguna duda al respecto. Ya se ha expuesto cómo la actuación en el conflicto armado de agentes no estatales incorpora una dificultad adicional cuando dicha participación se realiza a través de la red. Por este motivo, se tiene que reiterar la necesidad de que la atribución del hecho ilícito al Estado se base en criterios restrictivos, de forma que se evite, en la mayor medida posible, una respuesta inadecuada. En el caso de que un ciberataque armado lanzado por cibervoluntarios en el conflicto fuera incorrectamente atribuido a un Estado y se ejerciera la legítima defensa frente al mismo, podría ocurrir, asimismo, que la acción defensiva careciera de necesidad militar o resultara desproporcionada. Es decir, el Estado que no se encuentra librando un conflicto armado y sufre una

[813] En relación a estas cuestiones, pueden servir de ejemplo las reflexiones citadas de EYMAR ALONSO, C., *Estados Unidos y la cuestión de la legítima defensa preventiva*, y de GONZALEZ ALONSO, L.N., ¿Daños jurídicos colaterales? La invocación del artículo 42.7 del Tratado de la Unión Europea y la lucha contra el terrorismo internacional.

reacción defensiva por parte de otro que le atribuye inadecuadamente el hecho ilícito causado por cibervoluntarios será, de forma manifiesta, objeto de un ataque contrario al DIH.

La violación flagrante y sistemática de las normas de DIH será clara en los casos en que se ejerza la legítima defensa al margen de los requisitos que la legalidad internacional le impone. Cuando no exista la inicial agresión o el ilícito cibernético no revista tal carácter y cuando la respuesta sea desproporcionada es previsible que se cometa un acto de agresión de la índole de los recogidos en el artículo 8 del Estatuto. La falta de necesidad militar apuntada o la provocación de daños desproporcionados o innecesarios resulta evidente en estos casos. Asimismo, podría incurrirse en la violación de la obligación de distinguir objetivos civiles y militares si se actuara contra participantes civiles en el combate, entendiendo que los mismos lo hacen como agentes estatales.

Igualmente, en aras al respeto de la legalidad internacional, se impone la defensa del criterio de la temporalidad, pues cuando no se actúe de forma coetánea a la agresión cibernética que se sufre, nos podremos encontrar ante una agresión que incurra en ilicitud y que constituya, por sí misma, un ataque armado.

BIBLIOGRAFÍA BÁSICA CONSULTADA

LIBROS

AA.VV. El proceso hacia unas fuerzas armadas europeas: realizaciones y desafíos. Documentos de Seguridad y Defensa, núm. 55. Escuela de Altos Estudios de la Defensa, Ministerio de Defensa, marzo 2013.

AA.VV. Estrategia de la información y seguridad en el ciberespacio. Documentos de Seguridad y Defensa, núm. 60. Escuela de Altos Estudios de la Defensa. Ministerio de Defensa. Madrid. Junio 2014.

AA.VV. Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare. Program on Humanitarian Policy and Conflict Research at Harvard University. Berna.Mayo 2009.

AA.VV. (ed. Louise Doswald-Beck). San Remo Manual on International Law Applicable to Armed Conflicts at Sea. Prepared by a Group of International Lawyers and Naval Experts convened by the International Institute of Humanitarian Law, 1995.

ÇALIŞKAN, E., MINÁRIK, T., OSULA, A.M., Technical and Legal Overview of the Tor Anonymity Network. NATO Cooperative Cyber Defense Centre Of Excellence. Tallin 2015.

CARR, N., The shallows. What the internet is doing to our brains. Norton and Company Inc. New York, 2010.

HENCKAERTS, J.M. y DOSWALD-BECK, L., El Derecho Internacional Humanitario Consuetudinario, vol. I, Normas. Comité Internacional de la Cruz Roja, Buenos Aires, 2007

- Customary International Humanitarian Law, vol. II. Practice Part 1. International Committee of the Red Cross 2005.

- Customary International Humanitarian Law, vol. II Practice. Part 2. Cambridge University Press. 2005.

KALSHOVEN, F. y ZEGVELD, L. Restricciones en la conducción de la guerra. Introducción al derecho internacional humanitario. Comité Internacional de la Cruz Roja. Ginebra, marzo de 2001.

LABORIE IGLESIAS, M. La privatización de la seguridad. Las empresas militares y de seguridad privadas en el entorno estratégico actual. Instituto español de Estudios Estrategicos. Ministerio de Defensa. 2013.

LAWAND, K. CICR. Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos Medidas para aplicar el artículo 36 del PA I de 1977. Comité Internacional de la Cruz Roja Ginebra, enero de 2006. Comité Internacional de la Cruz Roja. Unidad Armas, División Jurídica.

MELZER, N., S., Interpretive Guidance on the notion of direct participation in hostilities. International Committee of the Red Cross, Ginebra 2009.

SALMÓN, E. Introducción al Derecho Internacional Humanitario. Instituto de Democracia y Derechos Humanos. Pontificia Universidad Católica de Perú. Comité Internacional de la Cruz Roja. Lima, 2012.

SANDOZ, Y., SWINARSKI, Ch., ZIMMERMANN, B. (Ed.). Commentary on the Additional Protocols to the Geneva Conventions of 8 June 1977 to the Geneva Conventions of 12 August 1949. International Committee of the Red Cross. Geneva, 1987.

SASSÒLI M., BOUVIER A. A., QUINTIN A. How does law protect in war? Cases, Documents and Teaching Materials on Contemporary practice in International Humanitarian Law. Part I, vol. I Outline of International Humanitarian Law. International Committee of the Red Cross.

- How does law protect in war? Cases, Documents and Teaching Materials on Contemporary practice in International Humanitarian Law. Part I, vol. II. Outline of International Humanitarian Law. International Committee of the Red Cross.

- Un droit dans la guerre ? Présentation du droit international humanitaire, vol. I, Seconde édition. CICR

- Un droit dans la guerre? Cas, documents et supports d'enseignement relatifs à la pratique contemporaine du droit international humanitaire, vol. I. CICR.

SCHMITT, M.N. (General Editor). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.

SINGER, P. W. and FRIEDMAN, A. Cybersecurity and cyberwar. What everyone needs to know. Oxford University Press. Oxford 2014.

TIKK, E. KASKA, K., VIHUL, L. *International Cyberincidents. Legal Considerations*. NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallin, 2010.

TIKK, E. KASKA, K., RÜNNIMERI, K., KERT, M., TALIHÄRM, A.-M., VIHUL, L. Cyber Attacks Against Georgia: Legal Lessons Identified. NATO Cooperative Cyber Defense Centre Of Excellence Publications, Tallin, 2008.

VERDROSS, A. Derecho Internacional Público. Biblioteca Jurídica Aguilar. Edición Española, 1973.

ZIOLKOWSKI K., Ius ad bellum in "Cyberspace – Some Thoughts on the "Schmitt- Criteria" for Use of Force. CZOSSECK, C. y otros, *2012 4th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn, 2012.

CAPÍTULOS DE LIBROS

BERMEJO GARCIA, R. ¿Puede la legitima defensa ponerse en un sitio? Algunos comentarios y reflexiones. Estudios de Derecho Internacional y de Derecho europeo en homenaje al Profesor Manuel Pérez González. Tomo I. Aznar Gómez, M., (Coordinador). Tirant lo Blanch. Valencia, 2012; pp. 209-236.

CÁCERES BRUN, J. *El sistema de eficacia del Derecho Internacional Humanitario*. Derecho Internacional Humanitario. (Coord. Rodríguez-Villasante y Prieto, J.L.). Cruz Roja Española. Centro de Estudios de Derecho Internacional Humanitario. Tirant lo Blanch. Valencia 2002; pp. 623-644.

CASANOVAS Y LA ROSA, O., *El Derecho Internacional Humanitario en los conflictos armados (I): Objetivos militares, métodos y medios de combate*. DIEZ DE VELASCO, M. Instituciones de Derecho Internacional Público. Tomo I, Tecnos. Madrid 2013; pp. 1097-1121.

CASANOVAS Y LA ROSA, O. *El principio de prohibición del uso de la fuerza*. Instituciones de Derecho Internacional Público. DIEZ de VELASCO, Tecnos, Madrid 2013; pp. 1067-1096.

DE LA HOZ CABALLER, J., Criminalidad y conflicto. Nuevas guerras nuevas paces. Monografias del CESEDEN núm. 131. Centro Superior de Estudios de la Defensa Nacional. Septiembre 2012; pp. 295-341.

DEWEESE, G.S., *Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence*. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace M. Maybaum, A.-M.Osula, L.Lindström (Eds.). NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn 2015; pp. 81-92.

DION, M., *Different Legal Constructs for State Responsibility*. International Cyber Security Legal & Policy Proceedings 2010. NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn, 2010; pp. 67-75.

DOMENECH OLMEDAS, J.L., La acción militar en las operaciones de paz. Estudios de Derecho Internacional y de Derecho europeo en homenaje al Profesor Manuel Pérez González. Tomo I. Aznar Gómez, M., (Coordinador). Tirant lo Blanch. Valencia, 2012; pp. 441-489.

ESPADA RAMOS, M.L., Nuevas formas de uso de la fuerza y su compatibilidad con el derecho Internacional actual". Estudios de Derecho Internacional Publico y Privado. Homenaje al Profesor Luis Sela Sampil. Universidda de Oviedo. 1970; pp. 301-323.

FARALDO CABANA, P., La responsabilidad por mando en el Código Penal español, en Olásolo Alonso, H., y Cuenca Curbelo, S., (Coords.), Perspectiva iberoamericana sobre la justicia penal internacional, vol.I, 2011, Valencia, 2012; pp.171-185

FELIU ORTEGA, L., La ciberseguridad y la Ciberdefensa. El Ciberespacio. Nuevo escenario de confrontación. CESEDEN. Monografías núm. 126, febrero 2012; pp. 35-69.

GARCÍA SEGURA, C., *Las iniciativas para la regulación de la actividad de las empresas militares de seguridad privada*. Las corporaciones privadas de seguridad. Plan Anual de Investigación 2015. Documento de trabajo 13/2015. Escuela Superior de las Fuerzas Armadas; pp. 14-38.

GÓMEZ DE AGREDA, A. *El ciberespacio como escenario del conflicto. Identificación de las amenazas.* El Ciberespacio nuevo escenario de confrontación. Monografías CESEDEN. Número 126. Febrero 2012; pp. 167-203.

GUISÁNDEZ GÓMEZ, J. *La protección de las víctimas en los conflictos de carácter no internacional*. Derecho Internacional Humanitario. (Coord. Rodríguez-Villasante y Prieto, J.L.). Cruz Roja Española. Centro de Estudios de Derecho Internacional Humanitario. Tirant lo Blanch. Valencia 2002; pp. 433-452.

HATHAWAY, M.E., and KLIMBURG; A. Preliminary considerations: on national cyber security. National cyber security framework manual. NATO Cooperative Cyber Defence Centre of Excellence. (Ed., Alexander KLIMBURG). Tallin 2012; pp.1-43.

HUGHES, R., *Towards a Global Regime for Cyber Warfare*. CZOSSECK, CH. and GEERS, K. (Eds.), The Virtual Battlefield: Perspectives on Cyber Warfare.IOSS Press. Amsterdam. 2009; pp.106-117.

JIMÉNEZ DE ARECHAGA, E., *La costumbre como fuente del Derecho Internacional*. Estudios de Derecho Internacional en Homenaje al profesor Miaja de la Muela. Vol. I.Tecnos. Madrid, 1979; pp. 375-402.

JUSTE RUIZ, J., *Las obligaciones erga omnes en Derecho Internacional Público*. Estudios de Derecho Internacional, Homenaje al Profesor Miaja de la Muela, T.I, Madrid, pp. 219 a 233.

MARÍN LÓPEZ, A., *Aspectos actuales de la responsabilidad internacional*. Estudios de Derecho Internacional. Libro-homenaje al Prof. A. Miaja de la Muela, Madrid, 1979, vol. II, pp. 815-836.

MIAJA de la MUELA, A., *Las situaciones jurídicas subjetivas en Derecho Internacional Público*. Estudios de Derecho Internacional Público y Privado. Homenaje al Profesor Luis Sela Sampil. Universidad de Oviedo. 1970; pp.25-50.

NIETO-NAVIA, R. *International Peremptory Norms (Jus Cogens) and International Humanitarian Law.* CASSESE, A., VOHRAH, L. C., Man's inhumanity to man: essays on international law in honour of Antonio Cassese. London 2003; pp. 595-640.

PÉREZ GONZÁLEZ, M., *La responsabilidad internacional (I): el hecho internacionalmente ilícito.* DIEZ DE VELASCO, M. Instituciones de Derecho Internacional Público. Tecnos, Madrid, 2013; pp. 843-871.

- *La responsabilidad internacional (II)*, en Instituciones de Derecho Internacional Público, Diez de Velasco, M. Tecnos. Madrid 2013.

PÉREZ NÚÑEZ, P.A., La paz y el fin de las narrativas. Nuevas guerras nuevas paces. Monografias, núm. 131. Centro Superior de Estudios de la Defensa Nacional. Septiembre 2012; pp. 17-66.

PIHELGAS, M. y PARK, G. *Cyber Information Exchange. Collaboration for Attribution of Malicious Cyber Activity*. PIHELGAS, M. (Ed.), Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks. NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallinn, 2015; pp. 8-23.

REGUEIRO DUBRA. R. *La aportación de la Corte Internacional de Justicia al concepto de legítima defensa*. El arreglo pacífico de controversias internacionales. VAZQUEZ GOMEZ, E.M.; ADAM MUÑOS, M.D.; CORNAGO PRIETO, N. (Coordinadores). Tirant lo Blanch. Valencia. 2013; pp. 185 a 204.

REMIRO BROTONS, A. *El crimen de agresión en el estatuto de la CPI revisado: nascetur ridiculus mus*. Estudios de Derecho Internacional y de Derecho europeo en homenaje al Profesor Manuel Pérez González. Tomo I. Aznar Gómez, M., (Coordinador). Tirant lo Blanch. Valencia, 2012; pp. 1115-1130.

SÁNCHEZ DE ROJAS DÍAZ, E. *Recursos vitales y recursos energéticos. Algunos conceptos básicos.* Recursos vitales y recursos energéticos. Implicaciones para la seguridad. Escuela de Altos Estudios de la Defensa. Monografías, núm. 141. Septiembre 2014; pp.19-62.

SHACKELFORD S. J., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Conference on Cyber Conflict Proceedings 2010 C. Czosseck and K. Podins (Eds.) NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallin, 2010; pp.197-208.

STINISSEN, J. A., *Legal Framework for Cyber Operations in Ukraine*. Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine. NATO Cooperative Cyber Defense Centre Of Excellence Publications. Tallin 2015; pp. 123-134.

VELÁZQUEZ ORTIZ, A.P., *Consideraciones sobre los ciberataques a la luz de los principios generales del empleo de las armas de conformidad con el Derecho Internacional Humanitario*. Seguridad y conflictos: una perspectiva multidisciplinar. VVAA. Miguel Requena (ED). Colección Investigación Instituto Universitario Gutiérrez Mellado. Madrid, 2012; pp. 435-463.

ARTÍCULOS

ABELLO-GALVIS, R. *Introducción al estudio de las normas de ius cogens en el seno de la Comisión de Derecho Internacional*, CDI. Universitas. Bogotá (Colombia) núm. 123, julio-diciembre de 2011; pp. 75-104**.**

ACOSTA ESTEVEZ, J.B., *Normas de ius cogens, efecto erga omnes, crimen internacional y la teoría de los círculos concéntricos*. Anuario de Derecho Internacional. 1995, vol. XI; pp. 3-22.

ADHAMI, W., *La importancia estratégica de Internet para los grupos armados insurgentes en las guerras modernas*. International Review of the Red Cross núm. 868. Diciembre de 2007; pp. 305-327.

AGUILAR CAVALLO, G., El reconocimiento jurisprudencial de la tortura y de la desaparición forzada de personas como normas imperativas de derecho internacional público, en Revista Ius et Praxis, vol.12, nº 1, Talca, 2006; pp.117-154.

ALLAN, C.S. *Attribution Issues in Cyberspace*, Chicago-Kent Journal of International and Comparative Law, vol. 13. Issue 2. 2013; pp.55-83.

AMICH ELIAS, C. y VELAZQUEZ ORTIZ, A.P. *La ciberdefensa y sus dimensiones global y específica en la Estrategia de Seguridad Nacional*. Revista ICADE, núm. 92

(Monográfico dedicado a: Seguridad y Defensa. Reflexiones a la luz de la Estrategia de Seguridad Nacional 2013); mayo-agosto 2014; pp. 50-76.

ANTOLIN-JENKINS, V. M., *Defining the parameters of cyberwar operations: looking for law in all the wrong places?* Naval Law Review 51, 2005; pp.132-174.

ARQUILLA, J. y RONFELDT, D., *Cyberwar is Coming!.* Comparative Strategy, vol. 12, No. 2, Spring 1993; pp.141–165.

BARBOZA, J., *Contramedidas en la reciente codificación de la responsabilidad de los Estados. Fronteras con la legítima defensa y el estado de necesidad*. Anuario Argentino de Derecho Internacional, vol. XII, 2003; pp.1-47.

BASSIOUNI, C., *International Crimes: Jus Cogens and Obligatio Erga Omnes*. Law and Contemporary Problems, vol. 59. Fall 1996; pp. 63-74.

BOLLO AROCENA M. D., *La responsabilidad internacional del Estado por la violación del Derecho Internacional Humanitario. A propósito de los hechos ocurridos en la cárcel de Abu Ghraib (Iraq).* Revista de Derecho Militar, núm. 86 Julio- Diciembre 2005; pp. 153-196.

BORREDA JUSTE, F., *Las armas químicas y biológicas. Respuestas al reto de la proliferación*. Documentos de Seguridad y Defensa, núm. 27. Centro Superior de Estudios de la Defensa Nacional. Marzo 2009; pp. 37-85.

BRENNER, S. W. with CLARKE, L. L., *Civilians in Cyberwarfare: Conscripts*. Vanderbilt Journal of Transnational Law, vol. 43; pp. 1011-1076.

BRILMAYER, L. y TESFALIDET, I. Y., *Third State Obligations And The Enforcement Of International Law*. International Law And Politics, vol. 44. 2011; pp. 2-56.

BROWN, G. y POELLET K., *The Customary International Law of Cyberspace*. Strategic Studies Quarterly. Fall 2012; pp. 126-145.

CÁNOVAS SÁNCHEZ, B. *Capacidades militares en temas NBQ-R. Las armas NBQ-R como armas de terror*. Monografías del CESDEN. Núm. 120. Centro Superior de Estudios de la Defensa Nacional. Mayo 2011; pp.141-197.

CARDONA LLORENS, J. *La responsabilidad internacional por violación grave de obligaciones esenciales para la salvaguarda de intereses fundamentales de la comunidad*

internacional. (EL «CRIMEN INTERNACIONAL»). Anuario de derecho internacional. VIII; pp. 265-336.

CARO BEJARANO, M. J., *Alcance y ámbito de la seguridad nacional en el ciberespacio. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. Cuadernos de Estrategia núm. 149. Instituto Español de Estudios Estratégicos. Instituto Universitario «General Gutiérrez Mellado». Diciembre 2010; pp. 49-82.

CHETAIL, V., *The contribution of the International Court of Justice to international humanitarian law*. International Review of the Red Cross. June 2003, vol. 85, no. 850; pp. 235-269.

CLAPHAM, A., *Obligaciones dimanantes de los derechos humanos para los actores no estatales en situaciones de conflicto*. International Review of the Red Cross, núm. 863 de la versión original. Septiembre de 2006; pp.2-37.

CLARK, R. S. *Amendments to the Rome Statute of the International Criminal Court Considered at the first Review Conference on the Court, Kampala, 31 May-11 June 2010.* Goettingen Journal of International Law, vol. 2, no. 2 (2010); 689-711.

COMELLAS AGUIRREZÁBAL, M.T., *La contribución del Consejo de Seguridad de las Naciones Unidas a la aplicación y al desarrollo normativo del Derecho Internacional Humanitario*. Revista Española de Derecho Militar, núm. 86; pp.175-212.

COLOM PIELLA, G y RODRÍGUEZ CHIRINO, C., *Construyendo la Ciberdefensa Aliada*. Revista de Aeronáutica y Astronáutica. Noviembre 2016; pp.926-931.

CONDRON, S. M., *Getting it right: protecting american critical infrastructure in cyberspace*. Harvard Journal of Law & Technology Volume 20, no. 2. Spring 2007; pp.404-422.

DE LUCCA, C.D., *The Need for International Laws of War to Include Cyber Attacks Involving State and Non- State Actors*. Pace International Law Review Online Companion. School of Law, vol. 3:9, enero 2013; pp. 278-315.

DE TOMÁS MORALES, S. y VELAZQUEZ ORTIZ, A.P., *La responsabilidad del mando en la conducción de operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz*». Revista Española de Derecho Militar núm. 100. Ministerio de Defensa, enero–diciembre 2013; pp. 117-150.

ECHEVERRI P., *Ius cogens en sentido estricto y en sentido lato: Una propuesta para fortalecer la consecución de la paz mundial y la garantía del Corpus Iuris Internacional de protección al ser humano*. Memorando de Derecho. Año 2 núm. 2. 2011; pp. 205-223.

FARWELL. J.P. y ROHOZINSKI, R. *Stuxnet and the Future of Cyber War*. Survival: Global Politics and Strategy 53:1, February –March 2011; pp.23-40.

FENRICK, W.J. *The rule of proportionality and Protocol I in conventional warfare*. Military Law Review vol. 98, Fall 198; pp. 91-127.

FERNANDEZ RODERA, J.A. *La lucha contra el delito en la red*. Cuadernos de la Guardia Civil núm. 51, 2015; pp. 112-123.

FOLTZ A.C., *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force! Debate*. JFQ issue 67, 4th quarter 2012; pp.40-48.

GEISS, R. *Las estructuras de los conflictos asimétricos.* Revista Internacional de la Cruz Roja núm. 864. Diciembre de 2006; pp. 1-23.

GILL, T. D and DUCHEINE, P. A. L., *Anticipatory Self-Defense in the Cyber Context. International Law Studies* vol., 89 U.S. Naval War College 2013; pp.438-471.

GONZÁLEZ CUSSAC, J. L., *Estrategias legales frente a las ciberamenazas.* Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia núm. 149. Instituto Español de Estudios Estratégicos. Instituto Universitario «General Gutiérrez Mellado». Diciembre 2010; pp. 79-127.

GROSSWALD, L., *Cyberattack Attribution Matters Under Article 51 of the U.N. Charter.* Brooklyn Journal of International Law vol. 36. Issue 3. 2011; pp. 1151-1181.

GUTIÉRREZ ESPADA, C., *La responsabilidad internacional del Estado por uso de la fuerza armada (la conformación del hecho ilícito internacional)*. Cursos de Derecho Internacional de Vitoria-Gasteiz, 1989. Servicio editorial de la Universidad del País Vasco, Bilbao, 1990; pp. 189- 310.

HATHAWAY, O. A. y otros. *The law of cyber-attack*. Yale Faculty Scholarship Series, paper 3852, 2012; pp. 817-886.

HEINSCH, R. *The Crime of Aggression After Kampala: Success or Burden for the Future?* Goettingen Journal of International Law 2. 2010; pp.713-743.

HENCKAERTS, J.-M., *Estudio sobre el derecho internacional humanitario consuetudinario: una contribución a la comprensión y al respeto del derecho de los conflictos armados*. Separata de la Revista Internacional de la Cruz Roja, vol. 87, núm. 857. Marzo de 2005; pp. 1-50.

HERNÁNDEZ GARCÍA, L. F., *Ciberseguridad; respuesta global a las amenazas cibernéticas del s. XXI. Las ciberamenazas, un nuevo reto para la Jefatura de Información de la Guardia Civil*. Cuadernos de la Guardia Civil núm. 49. 2014; pp. 5-35.

HOISINGTON, M. *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense.* Boston College International and Comparative Law Review vol. 32, 2009; pp.439-454.

HOLLIS, D.B., *Why States Need an International Law for Information Operations*. Lewis & Clark Law Review, Vol. 11. 2007, Temple University Legal Studies Research Paper No. 2008-43; pp.1023-1061.

JOYANES AGUILAR, L., *Estado del arte de la ciberseguridad*. Ciberseguridad. retos y amenazas a la seguridad nacional en el ciberespacio. Instituto Español de Estudios Estratégicos Instituto Universitario «General GUTIÉRREZ Mellado». Cuadernos de Estrategia, núm.149. Diciembre 2010; pp.13-46.

KASTENBERG, J.E., *Non-intervention and neutrality in cyberspace: an emerging principle in the national practice of International Law*. Air Force Law Review. Cyberlaw edition, vol. 64, 2009; pp.43-64.

KESAN, J.P. and HAYES, C. M., Self Defense in Cyberspace: Law and Policy. Illinois Public Law and Legal Theory Research Papers Series No. 11-16; pp. 1-36.

KILOVATY, I., *Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare*. National Security Law Brief 5, no. 1. 2014; pp. 91-124.

KRETZMER, D., *The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum*. European Journal of International Law, vol. 24, no. 1, 2013; pp. 235–282.

KYRIAKAKIS, J. *Developments in international criminal law and the case of business involvement in international crimes*. Business, violence and conflict. International Review of the Red Cross, vol. 94, no. 887. Autumn 2012; pp. 981-1005.

LIN, H., *Cyber conflict and international humanitarian law*. Humanitarian debate: Law, policy, action. New technologies and warfare. International Review of the Red Cross, vol. 94, no. 886. Summer 2012; pp.515-531.

LINDERFALK, U. *The Effect of* Jus Cogens *Norms: Whoever Opened Pandora's Box, Did You Ever Think About the Consequences?* The European Journal of International Law, vol. 18, no.5, 2008; pp. 853-871.

LOBEL, H., Cyber War Inc.: *The Law of War Implications of the Private Sector's Role in Cyber Conflict*. Texas International Law Journal, vol. 47, issue 3; pp.618-640.

LÓPEZ ALFRANCA, M. V., *¿Pero quién vigilará a los vigilantes?* Revista ICADE, núm. 92 (Monográfico dedicado a: Seguridad y Defensa. Reflexiones a la luz de la Estrategia de Seguridad Nacional 2013); mayo-agosto 2014; pp. 107-142.

LOTRIONTE, C., *Sovereignty and self-defense in cyber space*. Emory International Law Review, vol. 26. 2012; pp.826-919.

LUBELL, N. *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?* International Law Studies. U.S. Naval War College, vol. 89, 2013; pp. 252-275.

MARTÍNEZ ALCAÑIZ, A., *El Derecho Penal Internacional frente a los actos de terror acaecidos durante un conflicto armado*. Revista de Derecho Militar, núm. 102. Julio-Diciembre 2014; pp.89-127.

MATAMOROS MARTÍNEZ, R., *El marco jurídico del bioterrorismo*. Anuario Jurídico y Económico Escurialense, XXXVII (2004); pp. 17-46.

MAYORGA MARTÍN, J.L., *Hacktivismo*. Cuadernos de la Guardia Civil, núm. 49. 2014; pp. 36-53.

MEDLONG, J. *All Other Breaches: State Practice and the Geneva Conventions' Nebulous Class of Less Discussed Prohibitions*.Michigan Journal of International Law, vol. 34, issue 4.2013; pp. 829-856.

OTTIS, R., LORENTS, P., *Cyberspace: Definition and Implications*. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2010. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited; pp. 267-270.
PADMANABHAN, V. M., *Cyber Warriors and the Jus in Bello*. US Naval War College. International Law Studies, vol. 89, 2013; pp.288-308.

PAULUS, A. and VASHAKMADZE, M., *Asymmetrical war and the notion of armed conflict: a tentative conceptualization*. International Review of the Red Cross, vol. 91, no. 873. March 2009; pp. 95-125.

PERCY, S. *Regulating the private security industry: a story of regulating the last war*. International Review of the Red Cross, vol. 94, no. 887. Autumn 2012; pp.941-960.

PITERS, H. *Cyber Warfare and the Concept of Direct Participation in Hostilities*. NATO Legal Gazette. Legal issues related to cyber, issue 35. December 2014; pp.46-57.

QUESADA ALCALÁ, C., *El crimen de agresión como amenaza a la seguridad global. La respuesta del Derecho Internacional a los problemas actuales de la seguridad global.* Cuadernos de Estrategia, núm. 160. Instituto Español de Estudios Estratégicos. Cruz Roja Española-Centro de Estudios de Derecho Internacional Humanitario. Enero 2013; pp.77-116.

QUEVEDO RUIZ, J.R., *Naciones Unidas y la lucha contra la proliferación de las armas de destrucción masiva. Logros y expectativas. Naciones Unidas como principal elemento del multilateralismo del siglo XXI*. Monografías del CESDEN núm. 109. Centro Superior de Estudios de la Defensa Nacional. Febrero 2009; pp. 129-178.

QUINTEIRO BLANCO, M., *Consideraciones generales sobre las tecnologías de doble uso*. Tecnologías de doble uso en la industria de la Defensa. Cuadernos de Estrategia, núm. 67. Centro Superior de Estudios de la Defensa Nacional; pp.59-105.

QUISPE REMÓN, F. *Las normas de ius cogens: ausencia de catálogo*. Anuario español de Derecho Internacional, vol. 28, 2012; pp.143-183.
RABOIN, B. *Corresponding Evolution: International Law and the Emergence of Cyber Warfare.* Cleveland State Law Review, no. 31, 2013; pp. 603-688.

RATTRAY, G. J. and HEALEY, J., *Non -State Actors and Cyber Conflict. America's Cyber Future.* Security and Prosperity in the Information Age. Center for a New American Security, vol. II. June 2011; pp.65-86.

RENAUT, C., *The impact of military disciplinary sanctions on compliance with international humanitarian law*. International Review of the Red Cross vol. 90, no. 870. June 2008; pp. 319-326.

RICHARDSON, J. *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, 29 J. Marshall J. Computer*. Journal of Computer & Information Law, vol. 29, issue 1. Fall 2011; pp. 1-29.

RID, Th., *Cyber War Will Not Take Place*. Journal of Strategic Studies, vol. 35, no. 1 (febrero 2012); pp. 5–32,

RIOLA RODRÍGUEZ, J.M. *La situación actual de las tecnologías de doble uso*. Desarme y control de armamento en el siglo XXI: limitaciones al comercio y a las transferencias de tecnología. Cuadernos de Estrategia, núm. 169. Instituto Español de Estudios Estratégicos. Centro Superior de Estudios de la Defensa Nacional. Diciembre 2014; pp.157-191.

RODRÍGUEZ-VILLASANTE Y PRIETO, J. L., *La pérdida de la inmunidad de las personas civiles por su participación directa en las hostilidades*. Cuadernos de Estrategia, núm. 172. Instituto Español de Estudios Estratégicos; pp. 167-208.

SHACKELFORD, S. J. *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. Berkeley Journal of International Law. 192, 2009; pp. 193-250.

SÁNCHEZ DE ROJAS DIAZ, E. *¿Ciber…qué? La ciberseguridad., retos, riesgos y amenazas*. Revista Ejército núm. 837. Diciembre 2010; pp.136-143.

SÁNCHEZ GARCÍA, F., *El empleo de la fuerza en el conflicto asimétrico*. Revista Ejército, núm. 836. Diciembre 2010; pp. 22-30.

SÁNCHEZ RODRÍGUEZ, L.I., *Una cara oscura del Derecho Internacional: Legítima defensa y terrorismo internacional*. Cursos de Derecho Internacional de Vitoria-Gasteiz, 2002; pp.271-299.

SCHAAP, A.J. *Cyber warfare operations: Development and use under International Law.* Air Force Law Review, vol. 64, 2009; pp.121-174.

SCHMITT, M.N., *Cyber operations and the jus ad bellum revisited.* Villanova Law Review, vol. 56. Diciembre 2011; pp. 569-606.

- *Perfidy and protected status. Precision attack and international humanitarian law.* International Review of the Red Cross, vol. 87, no. 859 September 2005; pp.445-466.

- *Asymmetrical warfare and International Humanitarian Law.* Air Force Law Review, vol. 62, no. 1, 2007; pp. 2-42.

SCHMITT, M. N. & VIHUL, L., *Proxy Wars in Cyberspace.* Fletcher Security Review, vol. I, issue II. Spring 2014; pp.55-73.

SLIM, H. *Business actors in armed conflict: towards a new humanitarian agenda.* International Review of the Red Cross, vol. 94, no. 887, Autumn 2012; pp. 903-918.

TERRY, J. P., *The lawfulness of attacking computer networks in armed conflict and in selfdefense in periods short of armed conflict: what are the targeting constraints? The navy's EEO complaint pilot program.* Military Law Review, vol.169. September 2001; pp.70-91.

TORRES SORIANO, M. *Guerras youtube. El impacto de las nuevas tecnologías de la información en el tratamiento mediático de los conflictos armad*os. Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción. Instituto Español De Estudios Estratégicos. Centro Mixto Universidad De Granada-Mando De Adiestramiento y Doctrina Del Ejército De Tierra. Cuadernos de Estrategia, núm. 148. Agosto 2010; pp. 131 a 157.

VEDROSS, A. *Jus dispositivum and Jus cogens in International Law.* American Journal of International Law, vol. 60, 1966.; pp. 55-63.

VITÉ, S., *Typology of armed conflicts in international humanitarian law: legal concepts and actual Situations.* International Review of the Red Cross, vol. 91, no. 873. March 2009; pp. 69-94.

VON HEINEGG, W. H. *Territorial Sovereignty and Neutrality in Cyberspace.* International Law Studies. U.S. Naval War College, vol. 89, 2013; pp.123-156.

WATTS, S., *Combatant Status and Computer Network Attack*. Virginia Journal of International Law, vol.50, issue 2. 2010; pp. 392-447.

WAXMAN, M. C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*. Yale Journal of International Law, vol. 36, issue 2, 2011; pp.421-459.

WOUTERS, J. and VERHOEVEN, S., *The Prohibition of Genocide as a Norm of Ius Cogens and Its Implications for the Enforcement of the Law of Genocide*. International Criminal Law Review, vol. 3, 2005; pp. 401–416.

JURISPRUDENCIA

Jurisprudencia internacional

A) De la Corte Internacional de Justicia

Sentencias

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986.

Barcelona Traction, Light and Power Company, Limited, Judgment, I.C.J. Reports 1970.

United States Diplomatic and Consular Staff in Tehran, Judgment, I. C. J. Reports 1980.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Preliminary Objections, Judgment, I. C. J. Reports 1996

Reservations to the Convention of Genocide, Advisory Opinion : I.C. J. Reports 1951

Permanent Court of Internati

w (claim for indemnity) (merits): documents relating to judgment no. 13 (September 13th, 1928), fourteenth (ordinary) session (1928). Factory at Chorzow (Germ. v. Pol.), 1927 P.C.I.J. (ser. A) no. 9 (July 26).

GabCikovo-Nagymaros Project (HungarylSlovakia), Judgment, I. C. J. Reports 1997.

Corfu Channel case, Judgment of April 9th, 1949. I.C.J. Reports 1949.

w (claim for indemnity) (merits): documents relating to judgment no. 13 (September 13th, 1928), fourteenth (ordinary) session (1928).

Opiniones consultivas

Legal Consequences cf the Construction of a Wall in the Occupied Palestinian Territory,
Advisory Opinion, I. C. J. Reports 2004.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996.

Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, I.C.J. Reports 1971.

B) Tribunal Penal Internacional para la Antigua Yugoslavia

The Prosecutor v. Zoran KUPRE[KI], Mirjan KUPRE[KI], Vlatko KUPRE[KI], Drago JOSIPOVI], Dragan PAPI], Vladimir [ANTI], also known as "VLADO", IT-95-16-T, ITYC, 14 January 2000.
The Prosecutor v. Rajic, Case n. IT-95-12-R61, YCTY, September 1996.

Laudos arbitrales

Affaire des biens britanniques au Maroc espagnol Recueil des Sentences Arbitrales. Affaire des biens britanniques au Maroc espagnol (Espagne contre RoyaumeUni) 1er mai 1925. (II).

Jurisprudencia nacional

A) Sentencias de Tribunales extranjeros

The Essen Lynching Case TriaL of Erich Heyer and six others British Military Court For The Trial Of War Criminals, Essen, 18th-19th and 21 st-22nd, December, 1945.

Corte Suprema de Estados Unidos, caso *Yamashita,* decisión de 4 de febrero de 1946.

Supreme Court of Israel, Public Commitee against Torture in Israel v. Government of Israel, Case No. HCJ 769/02, 13 December 2006.

Trial of Otto Skorzeny And Others, General Military Government Court of the U.S. Zone of Germany 18th August to 9th September, 1947.The United Nations War Crimes Commission, *Law Reports of Trials of War Criminals*, vol. IX, 1949.

A-G Israel v. Eichmann (1968), 36 ILR 5 (Tribunal Distrital de Jerusalén).

Sentencias de Tribunales españoles

Sentencia núm. 1844/2000 del Tribunal Supremo (Sala de lo Penal), de 2 diciembre.

Sentencia núm. 104/2006 del Tribunal Constitucional (Sala Primera), de 3 abril de 2006.

Sentencia del Tribunal Supremo (Sala Tercera, de lo Contencioso-administrativo, Sección 6ª), de 31 Mayo de 1999.

DOCUMENTACIÓN

A) DOCUMENTOS NACIONES UNIDAS

Proyecto de artículos de responsabilidad internacional del Estado. Resolución aprobada por la Asamblea General, en su 56º período de sesiones [sobre la base del informe de la Sexta Comisión de Derecho Internacional de las Naciones Unidas. Doc. A/RES/56/83.

Comentarios al Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos. Aprobados por la Comisión de Derecho Internacional de las Naciones Unidas en su 53° período de sesiones (23 de abril a 1° de junio y 2 de julio a 10 de agosto de 2001). Asamblea General, Doc. A/56/10.

Resolución 2625 (1970), aprobada por la Asamblea General en su 1903ª sesión plenaria, de 24 de octubre 1970. Doc. A/RES/25/2625.

Resolución 3314 (1974), aprobada por la Asamblea General en su 2319ª sesión plenaria, de 14 de diciembre de 1974. Doc. RES/3314 (1974).

Resolución 55/63 aprobada por la Asamblea General en su 81ª sesión plenaria, de 22 de enero de 2001. Doc. A/RES/55/63.

Resolución 56/12, aprobada por la Asamblea General en su 88ª sesión plenaria, de 23 de enero de 2002. Doc. A/RES/56/121.

Resolución 57/239, aprobada por la Asamblea General en su 78ª sesión plenaria, de 20 de diciembre de 2002.Doc. A/RES/57/239.

Resolución 53/70, aprobada por la Asamblea General en su 79ª sesión plenaria de 4 de diciembre de 1998. Doc. A/RES/53/70.

Resolución 56/19, aprobada por la Asamblea General en su 68ª sesión plenaria, de 19 de noviembre de 2001. Doc. A/RES/56/19.

Resolución 58/32, aprobada por la Asamblea General en su 71ª sesión plenaria de 8 de diciembre de 2003. Doc. A/RES/58/32.

Resolución 62/17, aprobada por la Asamblea General en su 61ª sesión plenaria de 5 de diciembre de 2007. Doc. A/RES/62/17.

Resolución 64/211 aprobada por la Asamblea General en su 66ª sesión plenaria de 21 de diciembre de 2009. Doc. A/RES/64/211.

Resolución 1368 (2001), aprobada por el Consejo de Seguridad, en su 4370ª sesión, de 12 de septiembre de 2001. Doc. S/RES/1368 (2001).

Resolución 2249 (2015), aprobada por el Consejo de Seguridad en su 7565ª sesión, de 20 de noviembre de 2015. Doc. S/RES/2249 (2015).

Resolución RC/Res.6, aprobada por consenso en la 13ª sesión plenaria el 11 de junio de 2010. Anexo I. Enmiendas al Estatuto de Roma de la Corte Penal Internacional, relativas al crimen de agresión.

Tercer informe sobre la responsabilidad de los Estados de R. AGO, Doc. A/CN.4/246 y Add. 1 a 3.

Quinto informe sobre la responsabilidad de los Estados, por el Sr. Roberto Ago, Relator Especial. El hecho internacionalmente ilícito del Estado como fuente de responsabilidad internacional (*continuación*). Doc. A/CN.4/291 y Add.l y 2.

Adición al octavo informe sobre la responsabilidad de los Estados, por el Sr. Roberto Ago, Relator Especial, El hecho internacionalmente ilícito del Estado como fuente de responsabilidad internacional *(conclusión)*. Doc. A/CN.4/318/Add.5 a 7

Informe de la Comisión de Derecho Internacional, adoptado en su 66º período de sesiones (5 de mayo a 6 de junio y del 7 de julio al 8 de agosto de 2014). Doc. A/69/10. P. 296.

Primer Informe de la Comisión de Derecho Internacional sobre el *jus cogens*, Preparado por Dire Tladi, Relator Especial, presentado en el 68º período de sesiones (del 2 de mayo al 10 de junio y del 4 de julio al 12 de agosto de 2016). Doc. A/CN.4/693. P.26

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General. Seventieth sesión. Asamblea General. A/70/174. Distribuido el 22 de julio de 2015.

Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework. United Nations. Human Rights Office of the High Commissioner. New York and Geneva 2011.

Modelo de acuerdo sobre el estatuto de las fuerzas para las PKO entre Naciones Unidas y los países receptores fue recogido» en un Informe del secretario general de 9 de octubre de 1990 (Documento A/45/594, anexo).

International legal protection of human rights in armed conflict. United Nations publication. New York and Geneva, 2011.

A more secure world: Our shared responsibility. Report of the High-level Panel on Threats, Challenges and Change. United Nations 2004.

Documento de Montreux sobre las obligaciones jurídicas internacionales pertinentes y las buenas prácticas de los Estados en lo que respecta a las operaciones de las empresas militares y de seguridad privadas durante los conflictos armados. Anexo de la carta de fecha 2 de octubre de 2008 dirigida al Secretario General por el Representante Permanente de Suiza ante las Naciones Unidas, aprobada por la Asamblea General y el Consejo de Seguridad de Naciones Unidas, en su Sexagésimo tercer período de sesiones y Sexagésimo tercer año. Doc. A/63/467–S/2008/636.

B) DOCUMENTOS DE CRUZ ROJA

CICR, *El derecho internacional humanitario y los retos de los conflictos armados contemporáneos*. Informe resumido preparado por el Comité Internacional de la Cruz Roja resultante de la XXVII Mesa Redonda sobre problemas actuales del DIH: *Derecho Internacional Humanitario y otros regímenes jurídicos. Interacción en las situaciones de violencia*. Instituto Internacional de Derecho Humanitario, San Remo, Italia. Noviembre de 2003.

CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*. Informe resultante de la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja Comité Internacional de la Cruz Roja. Ginebra, Suiza octubre 2011.

CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*. Informe resultante de la XXXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Documento preparado por el Comité Internacional de la Cruz Roja. Ginebra, octubre de 2015.

CICR. *Empresas y Derecho Internacional Humanitario. Introducción a los derechos y las obligaciones de las empresas comerciales, de conformidad con el Derecho Internacional Humanitario*. Comité Internacional de la Cruz Roja. 2006.

CICR. *Armas nucleares y Derecho Internacional Humanitario*. Nota informativa número 4. Mayo 2013.

Second Expert Meeting on the Notion of Direct Participation in Hostilities. The Hague, 25 / 26 October 2004. Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees Expert Paper submitted by Michael N. Schmitt.

C) DOCUMENTOS DE OTAN

Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.

Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.

AJP-3.4.4 - Allied Joint Doctrine For Counterinsurgency.

NATO Civilian Affairs Committee. *Kosovo as a precedent: towards a reform of the Security Council?* International Law and humanitarian intervention. Arthur Paecht. General Rapporteur,16 de septiembre 1999.

D) OTROS DOCUMENTOS

Estrategia Española de Seguridad. Una responsabilidad de todos. Gobierno de España, 2011.

Estrategia Española de Seguridad Nacional. Estrategia de Seguridad Nacional. Un Proyecto Compartido, Presidencia del Gobierno, 2013.

Estrategia de Ciberseguridad Nacional, aprobada el 5 de diciembre de 2013 por el Consejo de Seguridad Nacional.

Strategy for Operating in Cyberspace, Department of the Army, 2011. Departamento de Defensa de los Estados Unidos.

Actualización de Internet II Metafísica. Centro de Análisis y Prospectiva. Gabinete Técnico de la Guardia Civil. Boletín actualidad internacional. Abril-Mayo 2015

Convenio sobre la Ciberdelincuencia. Informe Explicativo. Consejo de Europa. STE núm. 185.

Instructions for the Government of Armies of the United States in the Field (Lieber Code). 24 April 1863.

NATS System Failure 12 December 2014 – Final Report Independent Enquiry Final Report dated 13 May 2015. Authors: Robert Walmsley, Timothy Anderson, Clay Brendish, John McDermid, Martin Rolfe, Joseph Sultana, Mark Swan, Michael Toms.

Arreglo de Wasenaar sobre control de Exportaciones de Armas Convencionales y bienes y tecnología de Doble Uso, de 1996.

TRATADOS INTERNACIONALES

Carta de Naciones Unidas. San Francisco, Estados Unidos, el 26 de junio 1945.

Convención II de La Haya de 1899 relativa a las leyes y usos de la guerra terrestre y reglamento anexo.

Convenio IV de La Haya relativo a las leyes y costumbres de la guerra terrestre. 1907.

Convenio de Ginebra para mejorar la suerte de los heridos y enfermos de las fuerzas armadas en campaña. Ginebra, 12 de agosto de 1949. (BOE de 23 de agosto de 1952).

Convenio de Ginebra para mejorar la suerte de los heridos, enfermos y náufragos de las fuerzas armadas en la mar. Ginebra, 12 de agosto de 1949. (BOE de 26 de agosto de 1952).

Convenio de Ginebra relativo a la protección de los prisioneros de guerra. Ginebra, 12 de agosto de 1949. (BOE de 5 de septiembre de 1952).

Convenio de Ginebra relativo a la protección de personas civiles en tiempo de guerra. Ginebra, 12 de agosto de 1949. (BOE de 2 de septiembre de 1952).

Protocolo Adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales. (BOE de 26 de julio de 1989).

Protocolo Adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional. (BOE de 7 de octubre de 1989).

Tratado del Atlántico Norte. Washington D.C., 4 Abril de 1949.

Convención para la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de las Armas Químicas y sobre su Destrucción. París, 13 de enero de 1993.

Convención para la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de las Armas Biológicas (Bacteriológicas) y Tóxicas y de su Destrucción de 10 de abril de 1972.

Tratado sobre la No Proliferación de las armas nucleares, firmado en Londres, Moscú y Washington el 1 de julio de 1968.

Convenio de Viena sobre Relaciones Diplomáticas, de 18 de abril de 1961.

Convenio sobre la Ciberdelincuencia. Firmado en Budapest el 23 de Noviembre de 2001.

Convenio de Viena sobre el Derecho de los Tratados, de 23 de mayo de 1969.

Estatuto de la Corte Penal Internacional. Roma, distribuido como documento A/CONF.183/9, de 17 de julio de 1998, en vigor desde el 1 de julio de 2002.

Agreement between the Member States of the European Union concerning the status of military and civilian staff seconded to the institutions of the European Union, of the headquarters and forces which may be made available to the European Union in the context of the preparation and execution of the tasks referred to in Article 17(2) of the Treaty on European Union, including exercises, and of the military and civilian staff of the Member States put at the disposal of the European Union to act in this context (EU SOFA) (2003/C 321/02)". Diario Oficial de la Unión Europea, de 21 de diciembre de 2003.

LEGISLACIÓN NACIONAL

Código Penal. Ley Orgánica 10/1995, de 23 de noviembre. BOE núm. 281, de 24 de noviembre de 1995.

Código Penal Militar. Ley Orgánica 14/2015, de 14 de octubre. BOE núm. 247, de 15 de octubre de 2015

Ley Orgánica 2/2002 de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. BOE núm. 109, de 7 de mayo de 2002.

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. BOE núm. 109, de 7 de mayo de 2002.

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. BOE núm. 102, de 29 de abril de 2011. BOE

Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso. BOE núm. 312, de 29 de diciembre de 2007.

Instrumento de Adhesión de España al Convenio entre los Estados Partes del Tratado del Atlántico Norte relativo al Estatuto de sus Fuerzas, hecho en Londres el 19 de junio de 1951.BOE núm. 217, de 10 de septiembre de 1987.

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. BOE núm. 121, de 21 de mayo de 2011.

Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas. BOE núm. 33, de 7 de febrero de 2009.
Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Boletín Oficial de Defensa número 40, de 26 de febrero de 2013.

RECURSOS WEB

ARTEAGA, F. *La solidaridad española con Francia y el artículo 42.7 del Tratado de la UE*. Real Instituto Elcano. ARI 69/2015, de 23 de noviembre de 2015. Documento disponible en el sitio web: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/ari69-2015-arteaga-la-solidaridad-espanola-con-francia-articulo-427-tratado-ue.

AZNAR FERNADEZ DE MONTESINOS, F. *Terrorismo y estrategia asimétrica*. Documento de Opinión 9/2011. Enero de 2011. Instituto Español de Estudios Estratégicos. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO09_2011TerrorismoEstrategiaAsimetrica.pdf.

BENCSATH B., et al., *The Cousins of Stuxnet: Duqu, Flame, and Gauss*. Future Internet núm. 4, 2012. Disponible en el sito web: www.mdpi.com/1999-5903/4/4/971/pdf.

BEERLI, C., La privatización de la guerra: una perspectiva humanitaria. 14 de septiembre de 2012. Declaración de la 35º Mesa Redonda sobre Problemas Actuales de Derecho Internacional Humanitario. San Remo, 6-8 de septiembre de 2012. CICR. https://www.icrc.org/spa/resources/documents/statement/2012/privatization-war-statement-2012-09-06.htm.

CARLINI, A. *Isis: una amenaza en la era digital*. Instituto Español de Estudios Estratégicos. Documento de Opinión 129/2015. 1 de diciembre de 2015. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-2015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf.

CARO BEJARANO, M. J., *Flame: una nueva amenaza de ciberespionaje*. Documento Informativo 34/2012. Junio 2012. Instituto Español de Estudios Estrategicos. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI34-2012_Flame_Ciberespionaje_MJCB.pdf

CARO BEJARANO, M. J. *La protección de las infraestructuras críticas*. Documento de Análisis 021/2011, 27 de julio de 2011. Instituto Español de Estudios Estratégicos. Disponible en el sitio web:http://www.ieee.es/Galerias /fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf

CEBADA ROMERO, A. *Los conceptos de obligación erga omnes, ius cogens y violación grave a la luz del nuevo proyecto de la CDI sobre responsabilidad de los Estados por hechos ilícitos.* Revista Electrónica de Estudios Internacionales. Núm. 4. Junio 2002. Disponible en el sitio web:http://www.reei.org/index.php/revista/num4/agora/conceptos-

obligacion-erga-omnes-ius-cogens-violacion-grave-luz-nuevo-proyecto-cdi-sobre-responsabilidad-estados-hechos-ilicitos

CICR, *Guerra informática*, de 20 de octubre de 2010. Documento disponible en el sitio web: www.icrc.org/spa/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.

CICR, *La obligación de difundir el derecho internacional humanitario*. Servicio de Asesoramiento en Derecho Internacional Humanitario Febrero de 2003. Disponible en el sitio web: https://www.icrc.org/spa/assets/files/other/obligacion_difundir_dih.pdf.

CICR, *Guerra informática*, de 20 de octubre de 2010. Documento disponible en el sitio web: www.icrc.org/spa/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.

CICR. *Desafíos del DIH: el terrorismo*. Documento de 29 de octubre de 2010. Disponible en el sitio web: https://www.icrc.org/spa/war-and-law/contemporary-challenges-for-ihl/terrorism/overview-terrorism.htm

CICR. *La pertinencia del DIH en el contexto del terrorismo*. Documento de 1 de enero de 2011. Disponible en el sitio web: https://www.icrc.org/spa/resources/documents/misc/6fsjl7.htm.

CICR. *Derecho Internacional Humanitario y terrorismo: respuestas a preguntas clave*, Documento de 1 de enero de 2011. Disponible en el sitio web: https://www.icrc.org/spa/resources/documents/faq/5yyqg4.htm.

CICR, *Grave breaches specified in the 1949 Geneva Conventions and in additional Protocol I of 1977*. Documento de fecha 31 de enero de 1998. Disponible en el sitio web: https://www.icrc.org/eng/resources/documents/misc/57jp2a.htm.

CICR, *International Humanitarian Law and New Weapon Technologies*. Statement 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8-10 September 2011. Keynote address by Dr. Jakob Kellenberger, President, ICRC. Documento disponible en el sitio web: https://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm.

CCDCOE. Cyber Security Strategy Documents, disponible en el sitio web: https://ccdcoe.org/strategies-policies.html.

COLOM PIELLA, G. *¿El auge de los conflictos híbridos?* Documento de Opinión 120/2014. 24 de octubre de 2014. Instituto Español de Estudios Estratégicos. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO120-2014_GuerrasHibridas_Guillem_Colom.pdf.

DE SALVADOR CARRASCO, L., *Ciber-resiliencia*. Documento de opinión 35/2015. 3 de abril de 2015. Instituto Español de Estudios Estratégicos. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf

DENNING, D. E. *Stuxnet: What Has Changed?* Future Internet 2012, 4. Disponible en el sitio web: http://www.mdpi.com/1999-5903/4/3/672.

DEPARTAMENTO DE SALUD DE LOS ESTADOS UNIDOS, www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.

DROEGE, C. "*No hay lagunas jurídicas en el ciberespacio*", entrevista publicada en la web del CICR en fecha 16 de agosto de 2011. CICR. Disponible en el sitio web: https://www.icrc.org/spa/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

DOSWALD-BECK, L. *El derecho internacional humanitario y la Opinión consultiva de la Corte Internacional de Justicia sobre la licitud de la amenaza o del empleo de armas nucleares*. 31 de enero de 1997. Disponible en el sitio web: https://www.icrc.org/spa/resources/documents/misc/5tdldn.htm

EYMAR ALONSO, C., *Estados Unidos y la cuestión de la legítima defensa preventiva*. Grupo de Estudios Estratégicos. Disponible en el sitio web:http://www.gees.org/articulos/estados-unidos-y-la-cuestion-de-la-legitima-defensa-preventiva.

GONZALEZ ALONSO, L.N., ¿Daños jurídicos colaterales? La invocación del artículo 42.7 del Tratado de la Unión Europea y la lucha contra el terrorismo internacional. Documento disponible en http://www.reei.org/index.php/revista/num32/archivos/07_Estudio_GONZALEZ_LuisN.pdf.

INCIBE. *Jornadas Incibe Espacios Ciberseguridad*: https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes/programa-mi-ordenador-es-un-zombie

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATEGICOS. *Inventos del mundo militar que nos cambiaron la vida*. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/espacio_docente/Inventos_MundoMilitar_CambioVida.pdf.

GOBIERNO DE LOS ESTADOS UNIDOS, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information*, mayo de 2009. Documento disponible en el sitio web:https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pd.

KUTT NEBRERA, A., *La importancia de dominar los global commons en el siglo XXI*. Instituto Español de Estudios Estratégicos. Documento Marco 29/2012, de 12 de Noviembre de 2015. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf.

MANDO CONJUNTO DE CIBERDEFENSA. Boletín Informativo núm. 21 de 2016. *Ransomware.* Disponible en el sitio web: http://www.skalant.com/es/redes/23-ransomware-cuidado-con-el-secuestro-de-informacion.

McCORMACK, T.L.H., *Un non liquet con respecto a las armas nucleares. Revista Internacional de la Cruz Roja*. 31 de enero de 1997. Disponible en el sitio web: https://www.icrc.org/spa/resources/documents/misc/5tdlba.htm.

MELZER, N., *Cyberwarfare and International Law*. UNIDIR resources. 2011. Documento disponible en el sitio web: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

MINNIG, M., "*La protección de las personas en situaciones de violencia interna*". Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/america-internal-violence-itw-070708.htm

MOLINER GONZALEZ, J. *La cumbre de la OTAN en Varsovia*. Documento de Opinión 79bis/2016, de 2 de agosto de 2016. Instituto Español de Estudios Estratégicos. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO79bis-2016_CumbreOTAN_Varsovia_Moliner.pdf

MORENO FERNANDEZ, A.G., *La atribución al Estado de responsabilidad internacional por los hechos ilícitos de los particulares e intentos de flexibilización*. Revista Electrónica de Estudios Internacionales. Núm. 12.2006. Disponible en: :www.reei.org/index.php/revista/num12/archivos/MorenoFdez(reei12).pdf

NÚÑEZ PALACIOS, S. *El incumplimiento del Derecho Humanitario. Acciones internacionales.* 24 de febrero de 1999. Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/5tdmr6.htm

OSUJI, C. E., *Grave breaches' as war crimes: much ado about …'serious violations'*? Documento disponible en el sitio web: https://www.icc-cpi.int/NR/rdonlyres/827EE9EC-5095-48C0-AB04-E38686EE9A80/283279/GRAVEBREACHESMUCHADOABOUTSERIOUSVIOLATIONS.pdf

PALWANKAR, U. Measures available to States for fulfilling their obligation to ensure respect for international humanitarian law. International Review of the Red Cross. Documento disponible en el sitio web: https://www.icrc.org/eng/resources/documents/article/other/57jmaw.htm

PELLICER BALSALOBRE, J.M, El recurso humano en la doctrina para los escenarios de guerra asimétrica. Documento Marco 6/2017, 3 de abril de 2017. Instituto Español de Estudios Estratégicos. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_marco/2017/DIEEEM06-

PÉREZ BES, F., *El rol del abogado en la ciberseguridad*. Disponible en el sitio web:http://www.abogacia.es/2015/12/14/el-rol-del-abogado-en-la-ciberseguridad/

RAMIREZ MORAN, D., *La ciberseguridad en el contexto del Arreglo de Wassenaar*. Documento de análisis 16/2012. 9 de marzo de 2016. Instituto Español de Estudios Estratégicos. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_analisis/2016/DIEEEA162016_Ciberseguridad_Wassenaar_DRM.pdf

RAMÍREZ MORÁN, D. *La ciberdefensa en la Cumbre de Gales de la OTAN*. 13/2014. Instituto Estudios Estrategicos. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_informativos/2014/DIEEEI13-2014_Ciberseguridad_CumbreGales_DRM.pdf.

RAMÍREZ MORÁN, D., L*a visión internacional de la ciberseguridad*. Documento Informativo 2/2015, de 1 de abril de 2015. Instituto Español de Estudios Estratégicos. Documento disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf

REAL INSTITUTO ELCANO. *Las cibercelulas: una capacidad para la ciberseguridad y la Ciberdefensa nacionales*. ARI 26/2013, 4 de julio de 2013. Disponible en el sitio web:http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/ari26-2013-thiber-cibercelulas-ciberseguridad-ciberdefensa-nacionales

REGUEIRO DUBRA, R. *La Legítima Defensa en Derecho Internacional*. Instituto Universitario General Gutiérrez Mellado. UNED 2012. Disponible en el sitio web: http://iugm.es/wp-content/uploads/2016/07/la_legitima_defensa.pdf.

RICO RUIZ, E. *Nodo iNET: La comunicación permite a las Fuerzas Armadas mantenerse listas para actuar*. Disponible en el sitio web: https://www.bt.es/img/gestor/ministerio_defensa_red_internet_seguridad_IT.pdf

ROBLES CARRILLO, M. *El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico.* Documento de opinión 124/2015, 17 noviembre de 2015. Instituto Español de Estudios Estratégicos. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-Ciberseguridad_Margarita-Robles.pdf.

RODRÍGUEZ-VILLASANTE Y PRIETO, J.L. *Nota sobre la Conferencia de revisión del Estatuto de Roma de la Corte Penal Internacional, Kampala (Uganda), 2010*. Disponible en el sitio web:http://www.cruzroja.es/dih/pdfs/temas/3_4/3_4.pdf.

SÁNCHEZ HERRÁEZ, P. *La nueva guerra híbrida: un somero análisis estratégico*. Documento de Análisis 54/2014. 29 de octubre de 2014. Instituto Español de Estudios Estratégicos. Disponible en el sitio web: http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEEA54-2014_NuevaGuerraHibrida_PSH.pdf

SASSÒLI M., La responsabilidad del Estado por las violaciones del Derecho Internacional Humanitario. Revista Internacional de la Cruz Roja. Junio 2002. Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/5tecbx.htm.

SALA ORDOÑEZ, R., *NAT, autoría en ciberdelitos*. Documento disponible en el sitio web:http://www.abogacia.es/2016/03/14/nat-autoria-en-ciberdelitos/.

SCHMITT, M.N., *La guerra de la información: los ataques por vía informática y el ius in bello*. Revista Internacional de la Cruz Roja. 30 de junio de 2002. Disponible en el sitio web:https://www.icrc.org/spa/resources/documents/misc/5tecg3.htm.

- *International Law and cyber attacks: Sony v. North Korea*. Disponible en el sitio web: http://insct.syr.edu/wp-content/uploads/2015/06/Schmitt_International_Law_Cyber_Attacks.pdf

SPOERRI, P. "*Mesa redonda sobre el DIH y las nuevas tecnologías armamentísticas – Conclusiones*", de 13 de septiembre de 2011. Documento disponible en el sitio web:https://www.icrc.org/spa/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm

TAPIA ROJO, M.E., *Análisis de la estrategia comunicativa del terrorismo yihadista: el papel de las redes sociales*. Instituto Español de Estudios Estratégicos Documento de Opinión 02/2016. 4 de enero de 2016. Disponible en el sitio web:http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO02-2016_Comunicacion_ISIS_EugeniaTapia.pdf.

THE WHITE HOUSE. Office of the Press Secretary. Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea". Disponible en el sitio web: https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s.

ZIOLOWSKI, K. *Stuxnet-Legal considerations*. Cooperative Cyber Defense Centre Of Excellence. Tallin 2012. Documento disponible en el sitio web:https://ccdcoe.org/sites/default/files/multimedia/pdf/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf.