9.ª La noción de delito militar abarca no solo los definidos específicamente en la parte especial (Libro Segundo) como delitos militares, sino también aquellas conductas que infringen bienes jurídicos estricta o esencialmente militares incriminados en la legislación penal común, siempre que sean cualificados por la condición militar del autor y, además, por su especial afección a los intereses, al servicio y a la eficacia de la organización castrense.

10.ª Particularmente, se han coordinado determinadas conductas típicas para otorgar protección penal a los derechos fundamentales y libertades públicas reconocidas a los miembros de las Fuerzas Armadas por la Ley Orgánica 9/2011.

11.ª Ha presidido su redacción la necesidad de dar cumplimiento a las obligaciones convencionales asumidas por España, en particular relativas a la prevención y castigo de las violaciones del Derecho Internacional Humanitario, así como a las derivadas de la ratificación del Estatuto de la Corte Penal Internacional.

12.ª La regla general del Anteproyecto es que, en la situación de conflicto armado o estado de sitio, el delito tipificado en la Parte Especial del Código puede ser cometido cualquiera que sea la condición (militar o persona civil) del autor. Fuera de estas situaciones (supuestos de normalidad) se exige que el sujeto activo de los delitos previstos en el Código castrense tenga la condición militar. Y ello, sin perjuicio de la aplicación de las reglas sobre participación de *extraneus*. Sin embargo, excepcionalmente, fuera de aquellas situaciones puede ser sujeto activo del delito militar una persona civil, como en los delitos de allanamiento de dependencia militar (art. 29), desobediencia, resistencia o maltrato de obra a centinela (art. 34), inutilización voluntaria o simulación para eximirse del servicio (art. 61, párrafo segundo), delitos contra la Administración de la Justicia militar (art. 82), delitos contra el patrimonio si se tratare de material de guerra o armamento (art. 83.3) y la receptación (art. 88), todos ellos del Anteproyecto.

LA RESPONSABILIDAD DEL MANDO EN LA CONDUCCIÓN DE OPERACIONES DURANTE LA CIBERGUERRA: LA NECESIDAD DE UN ADIESTRAMIENTO EFICAZ

Susana De Tomás Morales
Ana Pilar Velázquez Ortiz

SUMARIO

1. INTRODUCCIÓN

Las nuevas tecnologías han supuesto una revolución en la vida cotidiana de millones de personas en el mundo que han visto cómo sus hábitos diarios se han transformado con el uso de las mismas. Las ventajas que la utilización de los medios telemáticos y cibernéticos han supuesto en el ámbito de las comunicaciones, de las transacciones comerciales o en el desarrollo de técnicas sanitarias resultan innegables. Sin embargo, también se ha podido constatar, en recientes incidentes, que el uso malicioso de estas tecnologías ha puesto en riesgo la seguridad de las personas y de los Estados a los que estas pertenecen y se ha revelado como una potencial amenaza para la Defensa Nacional y la Seguridad Internacional.

El uso de internet con fines bélicos no constituye hoy en día una posibilidad imaginaria, sino una oportunidad real. Por ello, se hace preciso analizar este medio desde el mismo prisma desde el que se estudian otras armas de guerra, en tanto que ha quedado comprobado que puede ser utilizado como tal. Una vez asumido este postulado, no puede obviarse que, como todo medio de combate, habrá de quedar sujeto a la regulación jurídica aplicable a los conflictos armados, para lo que, indefectiblemente, habrá que acudir al estudio del Derecho Internacional Humanitario (en adelante DIH).

En el sentido expuesto, el empleo de las redes informáticas supone una nueva configuración de los conflictos bélicos actuales que concierne no solo a las organizaciones internacionales y los Estados, sujetos de Derecho Internacional, sino que, de forma muy evidente, representa un gran reto para quienes, en primer lugar, están sujetos al respeto y aplicación de las normas en él contenidas: los Ejércitos en combate. Estos tienen, ante sí, un nuevo medio de guerra de cuya utilización responderán, en la manera en que el sistema de responsabilidad del mando queda articulado por el DIH.

El uso de las tecnologías con fines bélicos no reviste una única modalidad. Antes bien, el estudio de supuestos reales pone de relieve que nos encontramos ante lo que podrían considerarse tres categorías esenciales, determinantes para la calificación jurídica de los hechos. En consecuencia, el apartado segundo del presente trabajo atiende a las diversas manifestaciones de los mismos, distinguiendo entre los conceptos de ciberguerra, ciberoperaciones y ciberataques. Esta distinción implicará, necesariamente, una diversa respuesta por parte del DIH a cada una de las formas de uso del elemento cibernético. Las consecuencias de la inobservancia de las normas de DIH por parte del mando (civil o militar) se articularán siempre en función del principio de responsabilidad del mando definido por el DIH. Evidentemente, esta se exigirá tanto en el caso de que el mismo se halle conduciendo un conflicto armado cibernético o bien una ciberoperación en el transcurso de un conflicto armado convencional.

Por lo tanto, siendo ineludible la exigencia de dicha responsabilidad al mando de la operación de que se trate y teniendo en cuenta la novedosa y compleja materia que se aborda, cabe plantearse cuáles son los concretos elementos que, en el presente contexto, componen esta responsabilidad. En este sentido, el apartado tercero del trabajo examina la tradicional construcción de la teoría de la responsabilidad, elaborada a partir de las normas Convencionales y Consuetudinarias de DIH y, sobre todo, de las decisiones jurisprudenciales que se han considerado más ilustrativas. Dicho examen lleva a la conclusión de que los distintos elementos constitutivos de esta teoría resultan plenamente trasladables a los casos en que los crímenes

de guerra sean cometidos a través de operaciones conducidas por medios informáticos y que de ellos responderá quien se encuentre al mando de dichas operaciones. Esta responsabilidad será exigible, en consecuencia, tanto en el caso de que se ordene la comisión de crímenes de guerra, como en los supuestos en que el mando debiera haber conocido que los subordinados realizaban actividades de tal índole.

Trasladando pues la tradicional teoría a la nueva modalidad de combate, se pone de manifiesto la creciente importancia del adiestramiento en la materia, al objeto de cumplir con una de las esenciales obligaciones impuestas por el DIH en este aspecto, como es la de prevención de estos crímenes. El adiestramiento imprescindible en materia de DIH deberá, por lo tanto, incluir el elemento cibernético de forma que sea transmitido de una manera adecuada y eficaz a través de la cadena de mando.

Llegados a este punto, se hace necesario abordar el principio de responsabilidad indirecta (o por omisión) del mando en la conducción de las operaciones durante la ciberguerra. En relación con la responsabilidad por omisión, la necesidad de ofrecer y controlar el adiestramiento de los subordinados asume un protagonismo especial. Consecuentemente, será preciso atender a los elementos que integran el principio de la responsabilidad de mando por omisión. En este estudio se tendrá en cuenta tanto la ausencia de un adiestramiento como la insuficiencia del adiestramiento ofrecido a los subordinados, en claro perjuicio para la eficacia de la aplicabilidad de las operaciones cibernéticas, en situaciones, o no, de ciberguerra.

2. LA NUEVA CONFIGURACIÓN DE LOS CONFLICTOS

A pesar de que la alerta sobre el elemento cibernético ya se había puesto de manifiesto años antes[1], los ataques de esta naturaleza sufridos por Estonia y otras Repúblicas bálticas, en los años 2007 y siguientes, evidenciaron la fragilidad de la seguridad interna de esos Estados. La virulencia de esos ciberataques, la naturaleza de los objetivos que resultaron atacados, unido a la imposibilidad, prácticamente absoluta, de identificar a sus autores y llevarlos ante la justicia, hicieron que la doctrina internacional se planteara cuál había de ser la respuesta que, desde el punto de vista jurídico, debería darse a esta nueva forma de amenaza.

[1] 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», en CESEDEN, *El Ciberespacio. Nuevo escenario de confrontación,* Monografías, n.º 126, febrero de 2012, pp. 37-69.

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), cuyo patrocinio ha dado lugar a la publicación de *The International Law Applicable to Cyberwarfare,* también conocido como *Manual de Tallin.*

Naturalmente, el CIRC no ha permanecido ajeno a este debate. Desde un primer momento, se dejó sentado que, sin duda alguna, el DIH se aplica a los nuevos armamentos y tecnologías empleados en la guerra, tal y como se reconoce, en el artículo 36 del Protocolo Adicional 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»[2].

Sin embargo, 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[3].

2.1. La ciberguerra

La XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja[4] concluyó que uno de los desafíos para la aplicación del DIH, en relación con los conflictos armados contemporáneos, estaba constituido por lo que dio en llamarse ciberguerra. El documento resultante de dicha conferencia puso de relieve el hecho de que cualquier medio, conectado a internet, puede convertirse en un objetivo que puede ser atacado, desde cualquier parte del planeta. 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.

Aunque la delimitación entre ciberseguridad, ciberdefensa y ciberguerra ha querido trazarse de forma muy clara desde el principio por parte

[2] www.icrc.org/spa/resources/documents/interview/2011/cyber-warfare-interview.

[3] Schmitt, M. N., «La guerra de la información: los ataques por vía informática y *el jus in bello*», en *Revista Internacional de la Cruz Roja,* de 30 de junio de 2002, disponible en el sitio web http://www.icrc.org.

[4] La XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja se celebró en Ginebra, entre noviembre y diciembre de 2011, cuyos resultados pueden ser consultados en http://www.icrc.org/spa/index.jsp.

de la doctrina[5], en realidad, la línea que separa estos conceptos es a veces exigua y siempre difusa. 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. 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.

Para confirmar la existencia de un conflicto que pueda calificarse como ciberguerra, habrá que analizar, en primer lugar, la definición que el DIH proporciona de conflicto armado. El DIH distingue entre dos tipos de conflictos armados: los llamados internacionales, en los que se enfrentan dos o más Estados, y los no internacionales, entre fuerzas gubernamentales y grupos armados no gubernamentales, o entre esos grupos únicamente. Esta distinción se deriva 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 contenida en el artículo 1 del Protocolo Adicional II.

Desde el punto de vista jurídico, por tanto, 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 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, cuando son Estados los que 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

[5] En este sentido, Hathaway, M. E. y Klimburg, A., *Preliminary considerations: on national cyber security. National cyber security framework manual,* NATO Cooperative Cyber Defence Centre of Excellence, pp. 1-43. Disponible en http// www.ccdcoe.org.

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 Protocolo Adicional I amplía la definición de conflicto armado internacional a aquellos 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 (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 Protocolo Adicional 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.

La diferencia entre un conflicto armado en el sentido del artículo 3 común y otras formas menos graves de violencia, como las tensiones y los disturbios interiores, vendrá dada por el llamado umbral de enfrentamiento. Para determinar cuál haya de ser este, se utilizan generalmente dos criterios: por un lado, las hostilidades deben alcanzar un nivel mínimo de intensidad. Por otro, 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 tienen que estar sometidas a una cierta estructura de mando y tener la capacidad de mantener operaciones militares[6].

El artículo 1 del Protocolo Adicional II, ofrece una definición más restringida de conflicto armado no internacional, en tanto que este instrumento se aplica 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 operaciones militares sostenidas y concertadas y aplicar el presente Protocolo». Esta definición introduce la exigencia de control territorial, al establecer que las partes no gubernamentales deben

[6] Al respecto, puede consultarse: Comité Internacional de la Cruz Roja, Documento de opinión, elaborado en marzo de 2008. Documentación disponible en http://www.icrc.org/spa/assets/files/other/opinion-paper-armed-conflict-es.pdf.

ejercer un control territorial «que les permita realizar operaciones militares sostenidas y concertadas y aplicar el presente Protocolo». La restricción igualmente se fundamenta en el hecho de que el Protocolo Adicional 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 solo entre grupos armados no estatales.

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[7]. 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.

La obligación descrita 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 implementación del DIH se revelan esenciales en el desarrollo y conducción de los conflictos armados, ya se traten estos 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. El Centro de Excelencia de Ciberdefensa de OTAN, en su estudio *Cyberincidents. Legal considerations*[8], 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 este de haber desatendido

[7] En este sentido se expresa el Manual en su conjunto y más específicamente en su Norma 20. SCHMITT, M. *Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2013, pp. 68-70.

[8] TIKK, E. *International Cyberincidents. Legal Considerations,* Tallin (Estonia), 2010, pp. 36-47. Disponible en www.ccdcoe.org.

a las víctimas de la catástrofe de Chernóbil. En esas 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. No puede decirse que este caso desencadenara una ciberguerra, pero sí resulta ejemplificador de hasta qué punto, la ciberguerra puede desarrollarse como un conflicto no internacional.

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 Protocolo Adicional I. Esta declaración cumple la función adicional de contribuir a la constitución de un orden público internacional. En la actualidad, 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.

No puede obviarse, 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 del derecho humanitario, incluso, por parte de un tercer estado (en particular si este es parte en un conflicto armado).

Asumida, por tanto, la posibilidad de que nos encontremos ante una ciberguerra y dando por sentado que a la misma será de aplicación el DIH, es preciso traer a colación la definición del término «ataque», y examinar si resulta adecuada al nuevo contexto. El Protocolo Adicional 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 Protocolo Adicional 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 aquella que denota fuerza física[9]. Sobre la base de esta interpretación, las operaciones cibernéticas que, por medio de virus, causan un daño físico a las personas o los objetos más allá de los programas informáticos o los datos atacados, han de ser calificadas como «actos de violencia», es decir, ataques en el sentido del DIH. 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.

[9] En este sentido, es interesante la reflexión aportada por: HUGHES, R.,« Towards a Global Regime for Cyber Warfare», en Christian Czosseck y Kenneth Geers (eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare,* Ámsterdam, 2009, pp. 106-117.

> 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 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».

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 al desarrollo de los conflictos hasta ahora conocidos. Consecuentemente, estos ataques solo podrán dirigirse contra los objetivos militares y. por ende, los bienes civiles no podrán ser objeto de ataque, sin que la definición de objetivos militares dependa del tipo de guerra ante el que nos encontremos. Por lo tanto, el mando que dirigiera una operación hacia un objetivo civil, en el contexto de una ciberguerra, debería ser objeto de la exigencia de responsabilidad en virtud del DIH, de igual modo que lo hubiera sido en el caso de que ese objetivo civil se hubiera atacado en una guerra convencional.

El Protocolo Adicional I estipula no solo la aludida obligación de limitar los ataques estrictamente a los «objetivos militares» y de no dirigirlos contra la población civil o los objetos de carácter civil, sino también la prohibición de los ataques indiscriminados, esto es, aquellos que previsiblemente puedan causar víctimas o daños civiles incidentales, así como la obligación de 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).

La mención a 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 u objetivo presente 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 fáciles en su lanzamiento, conviene tener presente la absoluta aplicabilidad de esta norma.

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 ese 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.

De igual forma, el DIH prohíbe los ataques desproporcionados. En este sentido, se plantea la cuestión de 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 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 Protocolo Adicional 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 permiten[10].

[10] 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».

Por último, el Protocolo Adicional 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). De nuevo la cuestión relativa a la responsabilidad del mando vuelve a cobrar protagonismo. Las medidas tendentes a garantizar el respeto a estas normas pasan inevitablemente por la adecuada formación y adiestramiento del personal que le esté subordinado y haya de cumplir sus órdenes. En el aspecto que ahora se aborda resulta evidente que una inadecuada formación del personal encargado de la conducción de la ciberguerra podría conducir a la comisión de crímenes de guerra. Si el adiestramiento en materia de DIH resulta incuestionable en el ámbito de los conflictos tradicionales, con mayor motivo, debería ofrecerse a quienes sean responsables de la conducción de esta nueva modalidad de guerra.

2.2. Las operaciones cibernéticas

La naturaleza de los conflictos actuales conlleva que, en ciertos casos, las armas cibernéticas puedan utilizarse en combinación con operaciones cinéticas tradicionales. En este caso, la existencia de un conflicto armado es indudable y, por tanto, la aplicación del DIH resulta, igualmente, inexcusable.

Inicialmente, las operaciones cibernéticas fueron definidas[11] como aquellas que consisten en operaciones realizadas contra un ordenador o mediante un ordenador o un sistema informático, utilizando para ello el flujo de datos. De la amplitud de esta definición puede 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, este puede hallarse en manos casi de cualquier individuo, por lo que resultará especialmente necesario preservar la distinción entre civiles y combatientes a la que obliga el DIH.

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 con las ciberoperaciones que puede traerse a colación es la sufrida por Georgia en el año 2008. En este caso, 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 que este Estado sufrió. Como pone de manifiesto el Centro de Excelencia de OTAN en el estudio que realizó de este caso[12], todos los datos apuntan a que la ciberoperación fue lanzada por el Ejército ruso. Es incuestionable que la operación cibernética fue lanzada en un contexto bélico por cuanto Georgia se hallaba en situación de guerra (librada por medios que podemos llamar convencionales) con Rusia, como consecuencia de la contienda relativa a la región de Osetia.

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 infraestructuras críticas del enemigo. Por ello conviene recordar la imperatividad de las normas ya vistas en el apartado anterior de cuya observancia, responderá el mando de la ciberoperación. Esa

[11] *La XXXI Conferencia Internacional de la Cruz Roja …, op. cit.*

[12] TIKK, *Eneken. International Cyberincidents……*, doc. cit., pp. 66-89.

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[13] 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 del anonimato que garantiza el ciberespacio. Toda vez que, 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 aquel, el desconocimiento de dicha autoría, complica la labor de la atribución de una conducta. Todo ello dificulta la tarea de determinar la forma de aplicación del DIH a una ciberoperación.

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.

Por lo tanto, también en el ámbito de las ciberoperaciones, hay que resaltar la inexcusable aplicación del DIH, en virtud de la que los Estados y otras partes involucradas en un conflicto armado están obligados a respetarlo y hacerlo respetar. Esta obligación se extiende a los Estados y otras partes, que se ven compelidos 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.

La práctica de los Estados y de las organizaciones internacionales, respaldada por las conclusiones jurisprudenciales y la doctrina, en torno a la interpretación del artículo 1, común a los Convenios, lo configura como una norma de obligado cumplimiento «en todas las circunstancias», es decir, de forma incondicional y en ningún caso sujeta a la restricción de reciprocidad.

Es evidente, pues, la obligación para las Fuerzas Armadas de acatamiento del DIH. Conviene en este punto recordar que dicha norma no resulta imperativa exclusivamente en el desarrollo de operaciones en Territorio Nacional, sino también cuando dichas Fuerzas se encuentran en situación de combate en el extranjero[14]. Esta última situación puede producirse debi-

[13] *XXXI Conferencia Internacional…*, doc.cit.

[14] La decisión del Tribunal Penal Internacional para la antigua Yugoslavia (TPAY) en el caso «*Dusko*» *Tadic* ejemplifica el argumento expuesto, al dictaminar que un Estado

do a que las Fuerzas Armadas en cuestión se hallen en el contexto de operaciones de mantenimiento o establecimiento de la paz y con independencia de que esas operaciones se hayan emprendido directa o indirectamente por las Naciones Unidas. Cuando tales acciones son autorizadas por el Consejo de Seguridad de Naciones Unidas, las Fuerzas Armadas continúan bajo el mando y control del Estado al que pertenecen y, obviamente, la obligación de acatar el DIH, recae plenamente en ese Estado. No obstante, se impone a las Naciones Unidas el deber de asegurarse de que una operación que se desarrolle con su respaldo y conforme a sus intereses se lleve a cabo con arreglo a los dictados del Derecho Internacional, de forma que, como señala Pérez González, la Organización de Naciones Unidas, «viene a erigirse en una suerte de gendarme mundial de la paz»[15]. Los contingentes nacionales, que conforman dichas Fuerzas, siguen siendo entidades de su respectivo Estado, de manera que el Estado no renuncia al control sobre los mismos y mantiene, como mínimo, el «mando disciplinario» sobre su personal. Este vínculo, dispuesto de forma dual y complementaria, implica, por tanto, una responsabilidad de doble vía, en lo que respecta al acatamiento del DIH.

En definitiva, la obligación contenida en los Convenios de Ginebra es aplicable dondequiera que operen las Fuerzas Armadas de un Estado y no únicamente en el territorio de ese Estado[16]. Por lo que no cabe la menor duda de que la obligación de respetar y de hacer respetar los principios humanitarios en todas las circunstancias ha adquirido una categoría especial

es responsable de las violaciones del DIH cuando sus Fuerzas Armadas en el extranjero infringen las normas humanitarias o cuando los culpables, independientemente de su nacionalidad, son personas que actúan bajo el mando y control del Estado, incluso aunque no pertenezcan a sus Fuerzas Armadas. Esta decisión impone un control efectivo de carácter general y no considera necesario determinar, para cada violación, el control específico de un órgano del Estado en cuestión o la orden precisa emanada de dicho órgano. Judgement, *The Prosecutor vs. Dusko Tadic, Case n.º IT-94-I-A, ICTY Appeals Chamber,* 15 de julio de 1999.

[15] Pérez González, M. «Las Naciones Unidas y el mantenimiento de la paz: cincuenta años de esfuerzos». *Cuadernos de Historia Contemporánea,* n.º 17 (ejemplar dedicado a la Organización de Naciones Unidas), Servicio de Publicaciones. Universidad Complutense, Madrid, 1995, p. 61.

[16] La Sentencia del 14 de enero de 2000, del TPAY recalcó que «[como] consecuencia de su carácter absoluto, estas normas de derecho internacional humanitario no plantean obligaciones sinalagmáticas, es decir, obligaciones de un Estado respecto de otro Estado. Más bien [...] establecen obligaciones hacia la comunidad internacional en su conjunto, lo que tiene como consecuencia que cada miembro de la comunidad internacional tiene un "interés jurídico" en su observancia y, por consiguiente, tiene el derecho legítimo a exigir el respeto de dichas obligaciones». *The Prosecutor vs. Zoran Kupreskic and others, TPIY,* Sala de primera instancia, sentencia, La Haya, 14 de enero de 2000, caso no IT-95-16-T, párr. 519.

no solo en el derecho de las Naciones Unidas, sino también, de manera más general, en el orden jurídico internacional.

2.3. Los ciberataques

El cumplimiento de las normas establecidas en el DIH resulta 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 se han producido en este tipo de situaciones. Es el caso, por ejemplo, de los ciberataques que han sido objeto de examen en la publicación de OTAN *International Cyberincidents. Legal considerations.* Dejando al margen el supuesto ya visto de la ciberoperación de la que fue objeto Georgia y el ataque a bienes civiles en Bielorrusia, en la citada obra se atiende a los ataques sufridos por Estonia y 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 Estonia 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.

La misma reflexión puede hacerse en relación con el lanzamiento del virus STUXNET, (presuntamente por parte de Israel y Estados Unidos) contra las centrales nucleares de Irán, en el año 2010. 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[17].

[17] Al respecto, véanse: Gómez de Ágreda, A., «El ciberespacio como escenario del conflicto. Identificación de las amenazas», en *El Ciberespacio nuevo escenario de confrontación,* Monografías CESEDEN, n.º 126, febrero de 2012, pp. 202-203; y Joyanes Aguilar, L., «Introducción. Estado del arte de la ciberseguridad», en *Ciberseguridad. retos y amenazas a la seguridad nacional en el ciberespacio,* Instituto Español de Estudios Estratégicos Instituto Universitario «General Gutiérrez Mellado», Cuadernos de Estrategia,n.º 149, diciembre de 2010, pp. 13-46.

Sin embargo, atendidas la naturaleza y efectos de los ataques aquí planteados, 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, aquel en el que los primeros o los únicos actos «hostiles» se perpetran por medio de una operación cibernética. En este sentido, no parece aventurado afirmar que cualquier actividad, cometida por medios informáticos, que pueda ser asimilada a un acto hostil y produzca las mismas consecuencias que hubieran podido producirse por un medio convencional, pueda calificarse como susceptible de originar la aplicación del DIH. Con independencia de que el contexto en que se produzcan sea inicialmente bélico o no, a la vista del potencial del armamento cibernético, no puede descartarse que este origine un conflicto de aquella naturaleza. Por lo expuesto resulta plenamente factible que los ciberataques, de los que a diario se tiene constancia, puedan desencadenar una ciberguerra o, en su caso, un conflicto bélico de otra naturaleza que se inicie como consecuencia de que el Estado atacado responda a ese primigenio ataque, utilizando otros métodos de combate.

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 financiero 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 demoledores incluso en tiempo de paz y podrían originar el desencadenamiento de hostilidades.

En estos casos, no obstante, la exigencia de responsabilidad en el mando de una operación, sería sumamente difícil. En primer lugar porque habría que determinar si el ataque proviene de un componente de las Fuerzas Armadas de un Estado y, en ese caso, probar, igualmente, que el mismo actuaba cumpliendo una orden y no a título particular. Únicamente en el primer supuesto podría exigirse tal responsabilidad, condicionada, igualmente a que el Estado «atacante» asumiera esa actividad como propia, en cuyo caso nos encontraríamos ante el supuesto analizado en el apartado anterior[18].

[18] Renaut, C., «The impact of military disciplinary sanctions on compliance with international humanitarian law», en *International Review of the Red Cross*, vol. 90, n.º 870, junio de 2008, pp. 319-326.

3. EL PRINCIPIO DE LA RESPONSABILIDAD DEL MANDO EN LA CONDUCCIÓN DE LAS OPERACIONES DURANTE LA CIBERGUERRA.

El principio de la responsabilidad del mando atiende a la posibilidad de que los superiores puedan resultar responsables directos (cuando ordenan su comisión) o indirectos (cuando no impiden o no sancionan la conducta de los subordinados) de comisión de crímenes. Este principio tradicional del DIH, recogido en los artículos 86 y 87 del Protocolo Adicional I, ha sido internacionalmente consagrado, como lo demuestra su inclusión en el artículo 6 del Proyecto de Código de Crímenes contra la Paz y Seguridad Internacionales de la Comisión de Derecho Internacional (en adelante, CDI); en el artículo 28 del Estatuto de la Corte Penal Internacional (CPI); así como en los Tribunales Penales *ad hoc* constituidos para el enjuiciamiento de los crímenes cometidos durante los conflictos armados desarrollados en el territorio de la antigua Yugoslavia y de Ruanda (artículo 7 del TIPAY y 6 del TPR)[19].

El artículo 86.2 del Protocolo Adicional I dispone, como ya se ha comentado con anterioridad, que el hecho de que la infracción de las obligaciones que imponen los Convenios haya sido cometida por un subordinado no exime a los superiores de su propia responsabilidad por la supervisión y el control. En esta disposición se reconoce que la responsabilidad del mando incluye la obligación de garantizar que sus subordinados no comentan actos que impliquen violaciones graves del DIH. Dado que la conducta de los subordinados no ha de consistir en la comisión de una infracción calificada de «violación grave» del DIH, conviene recordar, siguiendo a Cherif Bassiouni, los elementos necesarios para que una infracción pueda ser calificada como tal:

> «1) Suponer una violación de prohibiciones en los Convenios o Protocolo I. 2) Encontrar cabida en el concepto de infracción grave de los artículos comunes 50/51/130/147 de los Convenios o artículos 11 u 85 del Protocolo I. Ellos exigen la concurrencia de un acto u omisión, y el hecho de que el afectado por la infracción sea una víctima o bienes protegidos contra infracciones graves»[20].

[19] El Consejo de Seguridad fue el impulsor, conforme a los poderes conferidos en virtud del Capítulo VII de la Carta de las Naciones Unidas, de la creación de sendos tribunales penales *ad hoc,* a través de la emisión de sendas resoluciones. El Tribunal Penal para la antigua Yugoslavia se creó a través de la Resolución 808, de 22 de febrero de 1993. El Tribunal Penal para Ruanda, mediante la Resolución 955, de 8 de noviembre de 1994.

[20] Cherif Bassiouni, M., *Derecho penal Internacional. Proyecto de Código Penal Internacional,* Madrid, 1984, p. 118.

Parece claro que las «infracciones graves» contenidas en los cuatro Convenios de Ginebra de 1949 y en su Protocolo Adicional I tendrían que verse incluidas en los estatutos de los tribunales penales internacionales mencionados. No en vano, como indicaba Pignatelli, las cuatro convenciones ginebrinas son normas de DIH y constituyen el núcleo aplicable en los conflictos armados, pues en cada una de esas convenciones «se contiene una disposición en que enumeran las infracciones que pueden considerarse "violaciones graves" o delitos de guerra»[21].

La responsabilidad del superior por crímenes de guerra, tal y como se deduce del contenido de los citados documentos, puede ser originada por una actuación directa o indirecta (por omisión)[22].

En el *Manual de Tallin* se atenderá también a ambos tipos de responsabilidad en la norma 24. En relación con la responsabilidad por omisión establecerá, en su apartado b) que:

> «El mando también es criminalmente responsable si conocía o debido a las circunstancias del momento debía conocer que sus subordinados estaban cometiendo o a punto de cometer o habían cometido crímenes de guerra y fracasa en tomar todas las medidas razonables y posibles para prevenir su comisión o castigar a los responsables».

Si tenemos en cuenta que la responsabilidad por omisión únicamente puede establecerse si el individuo que se ha abstenido de actuar tenía el deber de dicha actuación[23], debemos plantearnos si la ausencia o la inadecuación de un adiestramiento en la materia podría ocasionar la rendición de cuentas en virtud del principio de responsabilidad del mando por omisión[24]. Para ello se atenderá a los tres elementos[25] que componen el referido

[21] Pignatelli y Meca, F., «Consideraciones acerca del establecimiento del Tribunal Internacional para el enjuiciamiento de los presuntos responsables de violaciones graves del Derecho Internacional Humanitario cometidas en el territorio de la ex-Yugoslavia, a partir de 1991», en *Revista Española de Derecho Militar,* número 64, julio-diciembre, 1994; pp. 41-146 (en particular, p. 84).

[22] La naturaleza jurídica omisiva de este tipo de responsabilidad del mando fue establecida desde el conocido caso Yamashita.

[23] Véase Sandoz, Y. *et al.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 of 12 August 1949*, CICR-Martinus Nijhoff Publishers, Ginebra- Dordrecht, 1987, parágrafo 3537, p. 1010.

[24] Ejemplos de violaciones por omisión podemos encontrarlas, a modo de ejemplo, en el Protocolo Adicional I, arts. 44-45, 73, 75 y 85.

[25] Estos tres elementos han sido recogidos por las normas consuetudinarias y convencionales (artículos 86 y 87 del Protocolo Adicional I) de Derecho Internacional Humanitario; así como en los Estatutos de los Tribunales Penales Internacionales (en concreto, artículo 28 del Estatuto de la Corte Penal Internacional; artículo 7.3 del Estatuto del Tribunal Penal para la ex-Yugoslavia (TIPAY); y artículo 6.3 del Estatuto del Tribunal Penal para Ruanda (TPR).

principio: la existencia de un vínculo de subordinación, la obligación del saber del superior y la obligación del superior de actuar.

3.1. La existencia de un vínculo de subordinación

La exigencia de responsabilidad contenida en las normas del DIH, referidas tanto al personal civil como militar, impide que el mando u otros superiores eludan su responsabilidad criminal, cuando las ciberoperaciones constituyan un crimen de guerra, aunque estos no hayan cometido, personalmente, el acto que constituye tal crimen internacional.

Esta norma está contemplada en el Protocolo Adicional I y en los respectivos estatutos de la CPI y del TIPAY. Asimismo, se ha visto confirmada por la labor jurisprudencial desarrollada por el TIPAY[26], en varios asuntos sometidos en los que se incluyen, además de la investigación y la denuncia (objeto de atención en el punto 3.3.2 del presente estudio), los siguientes elementos:

a) Autoridad civil. Sobre la base de la responsabilidad de los superiores jerárquicos, la responsabilidad de los crímenes de guerra puede recaer, no solo en el personal militar, sino también en el civil.

b) Relación entre el superior y el subordinado. La relación entre el superior y el subordinado no ha de ser necesariamente directa, de *iure.* Basta la responsabilidad del superior de *facto.* Este principio se reconoce en varias sentencias emitidas por el TIPAY y el TPR. Estos Tribunales *ad hoc* han considerado que el criterio fundamental que hay tener en consideración es el control efectivo de los actos de los subordinados, en el sentido de la capacidad material de evitar que se cometan crímenes y castigar a los responsables. En el artículo 25 del Estatuto de la CPI se atiende a la misma noción.

c) Los jefes o mandos superiores sabían o deberían haber sabido. La práctica confirma que la responsabilidad no se limita a situaciones en las que el jefe o superior jerárquico tiene un conocimiento real de los críme-

[26] Se han desarrollado profundos estudios por parte de la doctrina en relación con esta labor jurisprudencial vinculada a la responsabilidad del mando, entre los que han de destacarse los siguientes: Domínguez Matés, R., «La doctrina de la responsabilidad del mando a la luz de la actual jurisprudencia del Tribunal Penal Internacional para la Ex Yugoslavia», en *Revista Española de Derecho Militar,* n.º 91, enero-junio de 2008; pp. 17-42; Pérez-León Acevedo, J. P., «La responsabilidad del superior *"sensu estricto"* por crímenes de guerra en el Derecho Internacional Contemporáneo», en *Revista Colombiana de Derecho Internacional,* n.º 10, Bogotá (Colombia), noviembre de 2007, pp. 153-198.

nes cometidos o que iban a cometer sus subordinados, sino que basta un conocimiento inferido. Esta noción se expresa en varias fuentes con formulaciones, ligeramente diferentes, que cubren, básicamente, el concepto de conocimiento inferido. Por lo que concierne a los superiores que no sean jefes militares, el Estatuto de la CPI emplea el siguiente lenguaje: «deliberadamente hubiere hecho caso omiso de información que indicase claramente [...]».

En el contexto de una ciberguerra, por tanto, se impone la responsabilidad criminal a cualquier mando militar u otro superior (incluidos civiles) que ordene ciberoperaciones que constituyan un crimen de guerra. Esta responsabilidad se extiende a través de la cadena de mando, de forma que el que ordena el cumplimiento de una orden emitida por un superior que implique cometer un crimen de guerra, resulta responsable de dicha orden y su ejecución. Así, el mando que reciba una orden y la traslade a sus subordinados para que lancen un ciberataque contra personas o lugares protegidos, será individualmente responsable de los ataques. Como ya se ha señalado, este tipo de responsabilidad sería directa. No obstante, este vínculo entre mando y subordinado se extiende a la responsabilidad indirecta o por omisión, cuando no se hayan adoptado las medidas de prevención, necesarias y razonables, para evitar la comisión del acto criminal por parte del subordinado.

Todo ello no viene más que a ratificar lo que en Derecho interno ya se contenía, al menos, en España. El Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas[27], en su artículo 56, al tratar la responsabilidad penal grave del mando militar, en relación con los delitos cometidos contra el Derecho Internacional Humanitario, taxativamente, establece: «Será consciente de la grave responsabilidad que le corresponde y asume para evitar la comisión, por las fuerzas sometidas a su mando o control efectivo, de los delitos de genocidio, lesa humanidad y contra las personas y bienes protegidos en caso de conflicto armado», sin que quepa, tampoco aquí, realizar interpretación alguna respecto de la plena aplicación de la norma transcrita.

El concepto de la responsabilidad que aquí se invoca fue establecido hace décadas en relación con los crímenes de guerra que, finalmente, se imputaron al General Yamashita[28]. Tras la Segunda Guerra Mundial, la Corte Suprema de los Estados Unidos sostuvo que el mencionado general

[27] *BOE, n.º 33, de 7 de febrero de 2009.*

[28] Corte Suprema de Estados Unidos, caso *Yamashita,* decisión de 4 de febrero de 1946.

fracasó en el ejercicio del «control efectivo» sobre algunas de sus fuerzas subordinadas, de forma que estas cometieron atrocidades que fueron consideradas crímenes de guerra. Entendió 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. Estos 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.

El artículo 28 del Estatuto de Roma establece una articulación contemporánea de este principio y prevé que el mando militar o la persona que actúe, de *facto,* como tal será criminalmente responsable por los crímenes que hayan sido cometidos bajo su efectivo mando o su efectiva autoridad y control, como resultado de su fracaso en ejercer el apropiado control sobre sus fuerzas. En el caso *Celebici,* el TIPAY se pronunciará sobre la posibilidad de establecer una relación de subordinación a través del ejercicio de mando de *facto:* « [...] individuals in positions of authority, whether civilian or within military structures, may incur in criminal responsibility under the doctrine of command responsibility on the basis of their *de facto* as well as *de iure* positions as superiors»[29]. No obstante, como se indicará en el referido caso, en la relación entre superior y subordinario se requiere, además, la existencia de una cadena de mando.

El principio de responsabilidad del mando, tal y como el DIH Consuetudinario pone de relieve, goza de una tradición y afianzamiento en la práctica que, difícilmente, podría verse alterada por el empleo de un específico método de guerra, por novedoso que este resulte. Sin embargo, ello lleva a incidir, una vez más, en la posibilidad de aplicación del DIH de carácter consuetudinario, y, en este específico supuesto, en la necesidad de adopción de medidas legislativas internas que faciliten la investigación de la autoría de los hechos que pudieran originar dicha responsabilidad.

Por otra parte, no debemos olvidar que son los propios jefes militares quienes han de garantizar que sus subordinados conozcan sus obligaciones a la luz de las normas del DIH, tal y como se recoge en el artículo 87.2 del Protocolo Adicional I. Ese control se efectuará teniendo en cuenta las responsabilidades que se derivan de los artículos 82 y 83 del referido Protocolo para los jefes de acuerdo a su grado de responsabilidad. Del contenido

[29] *Prosecutor vs. Delalic y otros (caso Celebici),* Caso IT-96-21-T, sentencia de 16 de noviembre de 1998; parágrafo 354.

de estos artículos, cabe concluir que tales criterios serán los aplicables a la instrucción de la tropa, de manera que el jefe de unidad será responsable de la instrucción de sus hombres, a través de los oficiales y suboficiales que se encuentren bajo su mando. En el ámbito que nos ocupa, el mando tendrá que garantizar que la necesaria formación en ciberoperaciones es recibida por el personal a sus órdenes, en la adecuada medida a sus concretas responsabilidades. Efectivamente, habrá que distinguir entre el adiestramiento que deba ofrecerse a la tropa en el teatro de operaciones del que deba darse a los responsables de la Sección CIS (Sistemas de Información y Telecomunicaciones). La labor de adiestramiento del mando, por tanto, se extiende a lo largo de toda su cadena de mando y, a la vez, se amplía en relación con este nuevo método de combate en el sentido de sensibilizar a todo subordinado que tenga a su alcance dicho método al objeto de que se evite la comisión de crímenes de guerra en el uso del mismo y, a la vez, esta pueda ser detectada en relación con los ataques que provengan de otros Ejércitos.

3.2. La obligación de saber del superior

El artículo 28 del Estatuto de la CPI exige este deber, aunque, como señala Pérez-León, desde distintos niveles de intensidad. Mientras que dentro del ámbito militar, como indica este autor, se puede generar responsabilidad del jefe militar «incluso por el simple deber de conocer *(should have known)*», mientras que fuera del ámbito castrense, «el Estatuto limita la responsabilidad exclusivamente a las conductas que implican una imprudencia consciente que va más allá de una mera imprudencia»[30].

El Derecho Internacional consuetudinario establece que «Los jefes y otros mandos superiores son plenamente responsables de los crímenes de guerra cometidos por sus subordinados si sabían, o deberían haber sabido, que estos iban a cometer o estaban cometiendo tales crímenes y no tomaron todas las medidas razonables y necesarias a su alcance para evitar que se cometieran o, si ya se habían cometido, para castigar a los responsables» (norma 153). Según se desprende de los comentarios a dicha norma es suficiente con que ese conocimiento sea un conocimiento inferido, como se ha querido dejar patente con la utilización de una variada terminología: «Tenían razones para saber», «[los superiores] sabían o poseían la información que les permitiera concluir, en las circunstancias del momento», «es

[30] Pérez-León Acevedo, J. P., «La responsabilidad...», *op. cit.*, p. 156.

responsable de no haber estado al corriente» y era «culpable de negligencia penal por no haber sabido»[31].

Este elemento fue objeto de atención por el TIPAY en el ya mencionado caso *Celebici,* atendiendo a las normas del Derecho Internacional consuetudinario. Sin embargo, resulta de especial interés su pronunciamiento en el caso *Blaskic,* en el que el TIPAY determinó que un superior siempre ha de estar informado sobre la manera en que sus subordinados desarrollan sus funciones, así como adoptar las medidas necesarias de prevención de crímenes internacionales[32].

Es evidente que, como se viene indicando, la complejidad técnica de las operaciones cibernéticas dificulta el conocimiento y alcance de las mismas[33]. Sin embargo, el hecho de que una ciberoperación pueda ser técnicamente complicada, no releva al mando o a cualquier otro superior de ejercer el control sobre sus subordinados. Desde el punto de vista jurídico, el mando militar deberá estar en posesión del mismo nivel de conocimiento que, razonablemente, pueda tener en otra operación que se desenvuelva en un contexto similar. En cualquier caso, el nivel de conocimiento ha de ser el suficiente para permitir que se cumpla con la obligación legal de actuar para identificar, prevenir o detener la comisión de un crimen de guerra cibernético. No se puede, por tanto, dejar de poner de relieve la necesidad de adiestramiento al mando militar y, por extensión, a todo participante en un conflicto bélico, de las previsiones del Derecho Internacional Humanitario y la necesidad de respetarlas, con independencia, nuevamente, del método de guerra que se emplee durante ese conflicto.

Como acertadamente apunta Domínguez Matés, el elemento clave a tener en consideración en relación con la responsabilidad del mando no radica en el conocimiento real que pudiera tener el superior, sino en «que su responsabilidad deriva de haber tenido "razones para conocer" a través de la información que, en virtud de su posición y según sus competencias, pudiera tener sobre lo que estuviera a punto de pasar o acabase de pasar»[34]. En relación con el tipo de información que pudiera tener el superior, esta autora, atendiendo a la labor jurisprudencial desarrollada por el TIPAY en el asunto *Naser Oric,* destaca la irrelevancia de la forma en la que sea

[31] Henckaerts, J. M. y Doswald-Beck, L., *El Derecho Internacional Humanitario Consuetudinario,* vol. I, Normas, Comité Internacional de la Cruz Roja, Buenos Aires (Argentina), octubre de 2007, pp. 632-636. Disponible en www.icrc.org.

[32] *Prosecutor vs. Blaskic,* caso IT-95-14T, sentencia de 3 de marzo de 2000, parágrafo 325.

[33] Véase al respecto Schmitt, M., «Rule 24. Criminal Responsibility of Commanders and Superiors», en *Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2013.

[34] Domínguez Matés, R., «La doctrina de la responsabilidad del Mando...», *op. cit.*, p. 33.

suministrada la misma al superior (oral u escrita) y ejemplos de cauces por los que los superiores pueden tener conocimiento de conductas de sus subordinados que pudieran derivar en la comisión de un crimen internacional. Entre estos ejemplos, el TIPAY incluirá «el grado de formación o entrenamiento del subordinado»[35], sus hábitos o el desarrollo de su carácter.

El deber de los estados de impartir cursos de formación en DIH a sus Fuerzas Armadas se encuentra recogido en las cuatro Convenciones de Ginebra de 1949 y en sus Protocolos Adicionales; en la Convención de la Haya para la protección de los bienes culturales y su Protocolo II; en la Convención sobre ciertas armas convencionales, especificando que dicha enseñanza se ha de aplicar tanto en tiempo de paz como en tiempo de conflicto armado; así como en la norma consuetudinaria número 142. Sin embargo, como se recoge en el comentario de la referida norma consuetudinaria, la práctica muestra «que no se exige que todos los miembros de las fuerzas armadas conozcan al detalle el derecho internacional humanitario, sino que basta con que sepan las normas esenciales del derecho que son pertinentes para sus funciones», por lo que la práctica seguida por los estados demuestra que «la mayor parte de la formación se imparte, principal o exclusivamente, mediante instrucciones escritas o en el aula, lo cual no siempre es suficiente para garantizar un cumplimiento eficaz en las complejas situaciones de combate [...] En circunstancias de combate, los soldados no suelen tener tiempo para pensar en los principios del derecho de los conflictos armados antes de actuar. Por lo tanto, no solo deben conocer esos principios, sino también recibir instrucción para que la respuesta apropiada en una situación específica sea espontánea»[36]. Si se relaciona esta obligación de los estados y la obligación de los superiores de tener un conocimiento sobre el grado de formación o entrenamiento de sus subordinados, es evidente que se extiende a la obligación de saber del superior si el adiestramiento recibido por sus subordinados es lo suficientemente eficaz como para aplicarlo en el desarrollo de las funciones que han de desempeñar en el contexto de operaciones cibernéticas.

Por otra parte, si el superior no estuviese seguro sobre el grado de suficiencia y eficacia del adiestramiento recibido por sus subordinados, debería contar con el asesoramiento jurídico apropiado. En este sentido, habría que recordar otra obligación estatal recogida en el artículo 82 del Protocolo Adicional I, alcanzando valor consuetudinario: «Cuando sea necesario, los

[35] *Prosecutor vs. Naser Oric,* Case IT-03-68-T, Judgement, 30 de junio de 2006, parágrafo 323.

[36] Henckaerts, J. M. y Doswald-Beck, L., *El Derecho Internacional....,* doc. cit., pp. 567-568.

estados pondrán asesores jurídicos a disposición de los jefes militares para que les aconsejen, al nivel adecuado, sobre la aplicación del derecho internacional humanitario» (norma consuetudinaria 141)[37].

En consecuencia, no se debería eximir de responsabilidad al superior que, teniendo conocimiento de la insuficiencia del adiestramiento recibido por sus subordinados, atendiendo al complejo campo (ciberoperaciones) en el que desarrollarán sus funciones, no actúe. El conocimiento del grado de suficiencia y eficacia debería ser evaluado por el propio superior, requiriendo, si fuese menester del correspondiente asesoramiento de los miembros del Cuerpo Jurídico Militar.

3.3. La obligación del superior de actuar

Si atendemos al párrafo 1 del artículo 87 del Protocolo Adicional I, relativo a los «Deberes de los jefes», se exige a los jefes militares que impidan las infracciones de los Convenios ginebrinos y del Protocolo y que, en caso necesario, repriman y denuncien dichas infracciones a las autoridades competentes. En cuanto al «deber de impedir» que incumbe a un superior, contenido en su párrafo 2, se requiere que los mandos tomen todas las medidas necesarias y razonables[38] para impedir su infracción y, en su caso, sancionar a los culpables. La ya mencionada norma consuetudinaria de DIH número 153 hace referencia a ese deber de impedir, al establecer que los jefes y otros mandos superiores son penalmente responsables de los crímenes de guerra cometidos por sus subordinados si no tomaron todas las medidas razonables y necesarias a su alcance para evitar que se cometieran.

Consecuentemente, debería determinarse, en primer lugar, si dentro de las medidas necesarias y razonables de prevención se podría incluir la ausencia o inadecuado adiestramiento en la materia que nos ocupa. Es decir, determinar si el superior tomó todas las medidas necesarias y razonables para impedir la comisión del acto delictivo: la comisión de un acto de ciberguerra que pueda ser incluido dentro de los actos prohibidos por el DIH.

[37] *Ibid.,* pp. 564-565.

[38] En el caso *Halilovic,* La Sala de Apelaciones del TIPAY entendió por «medidas necesarias» aquellas medidas adecuadas para que el superior cumpliera su obligación de impedir o castigar. Por su parte, consideró como «medidas razonables» aquellas que se encontraban razonablemente comprendidas en el ámbito competencial del superior. Véase: *Prosecutor v. Sefer Halilovic,* caso n.º IT-01-48-A, sentencia de 16 de octubre de 2007, parágrafos 63-64.

3.3.1. Medidas de prevención y adiestramiento

Si, como se ha mencionado en el apartado II del presente estudio, resulta un hecho innegable la aplicabilidad del DIH en las operaciones cibernéticas, la obligación de ofrecer un adiestramiento sobre la materia resulta evidente. Esta necesidad se revela obvia si tenemos en cuenta la población a la que habrá de dirigirse, constituida eminentemente por personal joven[39], con acceso a aplicaciones informáticas de última generación, de las que pueden hacer uso, a veces negligente, a través a de sus teléfonos móviles particulares.

En este sentido, deberíamos atender, una vez más, al Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas[40]; en especial, su Capítulo VI «De la ética de las operaciones», en el que se 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[41] (artículo 106, bajo el título «Deberes en relación con el Derecho Internacional Humanitario»). Con independencia de la desafortunada ausencia de referencia alguna a las normas consuetudinarias de DIH, el artículo 106 nos permite deducir que en cualquier conflicto armado, incluida la ciberguerra, así como en cualquier operación militar, incluidas las operaciones cibernéticas de seguridad y de defensa, deben aplicarse las normas oportunas del DIH. Ante este deber cabe interrogarse sobre cuáles serían las medidas necesarias y razonables de prevención de infracciones de las normas de DIH en el contexto de una ciberguerra o de cualquier operación cibernética. Sin lugar a dudas la respuesta no puede ser otra más que la de ofrecer un adiestramiento adecuado.

La obligación de difundir las normas pertinentes de DIH, se encuentra recogida en el artículo 83 del Protocolo Adicional I, estableciendo que:

[39] Atender a los factores de los subordinados resulta necesario, pues, como nos recuerda Bantekas, la Corte Militar Canadiense, establecida en Aurich (Alemania), caso *Canadá vs. Kart Meyer,* (veredicto del 28 de diciembre de 1945, p. 162) determinó que los superiores pueden ser considerador responsables por la conducción de sus subordinados, si fallan en tomar en consideración factores que podrían haberles indicado conclusiones obvias, como por ejemplo: la edad, el entrenamiento o experiencia de sus subordinados. Véase BANTEKAS, I., "The contemporary law of superior responsibility", en *American Journal of International Law,* vol. 93, n.º 2, 1999, p. 593.

[40] .Véase n. 27, *supra.*

[41] En concreto, se hace 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».

> «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».

Si esta primera dimensión del deber de prevenir la comisión de crímenes de guerra de los subordinados (artículo 86.2[42] del Protocolo Adicional I; artículo 7.3 del Estatuto del TPAY y artículo 6.3 del Estatuto del TPR[43]), incluye la obligación de difundir las normas pertinentes de DIH, el segundo interrogante a resolver será el atender a la adecuación de dicho adiestramiento.

Como ya se ha señalado, las operaciones cibernéticas pueden ser incluidas dentro de los medios y métodos de combate prohibidos por el DIH, pudiendo ocasionar males superfluos o sufrimientos innecesarios o estar dirigidos a producir graves perjuicios al medio ambiente, a la salud o, incluso, a la propia supervivencia de la población. Por otra parte, la obligación de no utilización de estos medios y métodos de combate se recoge en el artículo 114 de las Reales Ordenanzas para las Fuerzas Armadas[44], como otra obligación incluida en la ética de las operaciones. Si atendemos, además, a las características propias de esta nueva arma de guerra y al acceso generalizado de las redes militares a la gran mayoría de los miembros de las Fuerzas Armadas, se requiere que dicho adiestramiento sea ofrecido, con carácter general, desde su incorporación, formando parte de los planes de estudio de todas las Academias castrenses y demás centros de formación. El tomar estas medidas necesarias y razonables desde el momento mismo del ingreso en el correspondiente centro de formación nos hace reflexionar sobre el momento en el que comienza el deber de prevención. Al efecto, se puede recordar cómo en el ya mencionado caso *Yamashita,* se

[42] Si no tomaron todas las medidas factibles que estuvieran a su alcance para impedir, es infracción.

[43] El artículo 6.3 del Estatuto del TPR establece la responsabilidad penal del superior si «(...).no adoptó las medidas necesarias y razonables para impedir que se cometieran (...)».

[44] Véase n. 27, *supra.*

determinó que el deber de prevenir un crimen comienza cuando los mandos tienen una sospecha razonable sobre la comisión de crímenes de guerra por parte de sus subordinados, abarcando la responsabilidad del superior un deber de controlar a sus tropas, incluso antes de que el deber de prevención comience[45]. En ese caso, la Corte estadounidense constató el fracaso del control por parte del general Yamashita, al no inspeccionar personalmente a sus tropas. En parangón, podríamos deducir que se incluye, en la responsabilidad del mando, la función de controlar que el adiestramiento que se ofrece a los subordinados resulta adecuado.

Sin embargo, se planta un interrogante: ¿cómo puede considerarse adecuado un adiestramiento en una materia tan relevante como la que nos ocupa? La adecuación deberá conseguirse a través de dos vías que, por su conexión, no podrán ser paralelas, sino concurrentes. En primer lugar, habrá que formar al subordinado en materias de DIH. Esta es una labor que hasta ahora ha sido muy tenida en cuenta por los mandos de las Fuerzas Armadas, pero en este momento, deberá incluir la materia que nos ocupa por constituir un nuevo medio de combate. Pero, adicionalmente, cuando se ofrezca la capacitación necesaria para el desarrollo técnico de las ciberoperaciones, será necesario alertar a quien haya de ordenarlas y conducirlas materialmente de que el empleo de esta técnica queda sujeto a las normas de DIH.

No obstante, como apunta Bantekas, los superiores pueden descargar su responsabilidad respecto al deber de prevención si emplean todos los medios a su alcance para cumplir con esa obligación[46]. Consecuentemente, si se han tomado las medidas necesarias y razonables para ofrecer un adiestramiento adecuado, el superior podría eximirse de responsabilidad por omisión, en el sentido que nos ocupa.

3.3.2. Investigación y denuncia

Como se ha señalado con anterioridad, la investigación y denuncia constituye otro elemento esencial de la responsabilidad del mando. El hecho de que no se castigue a los subordinados que cometen crímenes de guerra puede deberse a que los presuntos crímenes de guerra no se investigan o no se denuncian a las autoridades superiores, como se establece en el Protocolo Adicional I y en el Estatuto de la CPI. En su sentencia en el

[45] *Corte Suprema de Estados Unidos...*, doc. cit., p. 327.
[46] Bantekas, I., «The contemporary...», doc. cit., p. 591.

caso *Blaskic,* el TIPAY puntualizó que un jefe debe dar prioridad, cuando sepa o tenga razones para saber que sus subordinados van a cometer un crimen, a evitar que lo cometan y que «no puede subsanar su omisión de actuar castigando después a los subordinados». En la referida sentencia, el Tribunal sostuvo que «en algunas circunstancias, un jefe puede cumplir su obligación de evitar o castigar un delito, comunicando el asunto a las autoridades competentes».

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[47].

De acuerdo con lo previsto en esta normativa, el mando militar u otro superior que conozca que una operación cibernética puede haber producido el resultado de un crimen de guerra está obligado a tomar medidas para asegurar que dicho crimen es investigado de la forma más adecuada, siempre teniendo en cuenta las circunstancias concurrentes. Asimismo, está obligado a informar a las autoridades judiciales y a aquellas que resulten competentes para investigar. Sin embargo, como señala Tikk, en la práctica totalidad de los ciberataques estudiados por OTAN se comprobó que, incluso estando previstas en los respectivos Códigos Penales las actividades cometidas, la legislación procesal resultó insuficiente para dar respuesta a las especiales necesidades de indagación de la autoría de los mismos[48]. En concreto, la Ley de Vigilancia de Estonia, de 22 de febrero de 1994, impedía el análisis de transmisión de datos, al tiempo que la Ley Procesal solo otorgaba validez a las pruebas, siempre que estas hubieran sido recogidas

[47] 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.
[48] Tikk, E. *International Cyberincidents..., op. cit.*

para la investigación de un delito y de un hecho concreto, sin permitir una investigación de carácter colectivo o general.

En relación con la materia objeto de atención en el presente estudio, resulta especialmente relevante la obligación de «poner en conocimiento de las autoridades competentes», recogida en el Estatuto de la CPI. Obligación que permite su extensión a superiores sin poder disciplinario o de sanción penal de un crimen. Esta obligación ya fue objeto de regulación en el artículo 87.1 del Protocolo Adicional I, aunque referido a la obligación de denunciar (o deber de informar). Esta obligación está dirigida a denunciar o poner en conocimiento de las autoridades competentes la comisión de un crimen por un subordinado. Sin embargo, si el superior es conocedor de la inexistencia o la inadecuación de un adiestramiento eficaz en las normas de DIH durante la conducción de operaciones en el desarrollo de una ciberguerra, ¿está obligado a informar al respecto por considerar que dicha carencia o inadecuación puede originar la futura comisión de un crimen de guerra?

Si las medidas preventivas (necesarias y razonables) que han de tomarse dependen del caso concreto (ciberataque como arma de guerra), habrán de ser consideradas de forma diferente, atendiendo a si el crimen aún no se ha consumado o si ya se ha cometido, en cuyo caso las medidas necesarias y razonables serían ya de carácter punitivo. La obligación de informar ¿podría extenderse tanto a las medidas preventivas como punitivas? En relación con las operaciones cibernéticas y la necesidad de ofrecer un adiestramiento eficaz, parece ser necesaria la extensión de la obligación de «poner en conocimiento de las autoridades competentes» tanto las medidas preventivas como punitivas. No debemos olvidar, siguiendo a Pérez-León, que el deber de prevenir «debe basarse en la verosimilitud de que los crímenes de guerra ocurran»[49], en el sentido de que no puede ser exigido sobre la base de una predicción de la conducta de los subordinados, sin la existencia de indicios que puedan llevar a la comisión de infracciones graves del DIH.

En cualquier caso, tanto las medidas de prevención como de sanción son necesarias, sin olvidar, como estableció el TPR en el caso *Bagilishema*[50], que no podrá ser compensada la ausencia de medidas preventivas

[49] Pérez-León Acevedo, J. P., «La responsabilidad...», *op. cit.*, p. 192.

[50] El TPR determinó que «(...) l'obligation faite au supérieur d'empêcher ou de punir le crime ne place pas l'accusé face à plusieurs options. Ainsi le supérieur qui savait ou avait des raisons de savoir que ses subordonnés étaient sur le point de commettre des crimes et qui ne les en a pas empêchés ne peut-il compenser ce manquement en punissant après coup les dits subordonnés» *Prosecutor vs. Bagilishema*, caso ICTR-95-1-T, sentencia del 7 de junio de 2001, parágrafo 49.

necesarias y razonables con medidas de sanción. Consecuentemente, no se puede olvidar que la obligación de ofrecer un adiestramiento eficaz constituye un elemento nuclear dentro de las medidas de prevención necesarias para evitar la comisión de crímenes de guerra. Por lo tanto, el principio de responsabilidad del mando no podrá ser suficientemente atendido si se obvia el aludido elemento relativo a la necesidad deadiestramiento.

4. CONCLUSIONES

Del examen realizado se concluye que la posibilidad de que una ciberguerra se declare en un futuro no excesivamente lejano hace que el régimen jurídico aplicable a esta haya de quedar clarificado de antemano. Ello pasa por la ineludible aplicación del DIH. Vista la definición de conflicto que aporta el DIH, resulta evidente que la ciberguerra no es sino una modalidad de este, y ello implica que serán las normas de DIH las que determinen el modo en que ha de conducirse un conflicto cibernético y las limitaciones que se impongan al mismo, así como la responsabilidad exigible al mando de aquel. Es evidente que, con independencia del tipo de combate que se libre, el personal al mando del mismo responderá de la comisión de los crímenes de guerra que pudieran cometerse en su transcurso. Por lo tanto, el personal al mando de una ciberguerra deberá ser consciente de que la distinción entre objetivos civiles y militares tiene la misma vigencia que en la guerra que podría denominarse convencional. De igual forma se le impide la realización de ataques desproporcionados, o de aquellos que causen daños indiscriminados, por cuanto la producción de los mismos es tan posible con la utilización de armas virtuales que con el uso de otras armas de guerra.

Por ello, habida cuenta de los distintos elementos de la teoría de la responsabilidad del mando, el adiestramiento en la materia resulta imprescindible. Dar a conocer al mando la trascendencia y consecuencias que pueden llegar a tener las órdenes que el mismo emita en la conducción de una ciberguerra, es tan necesario como que él mismo ofrezca ese adiestramiento al personal que se encuentre a sus órdenes. Únicamente así podrá decirse que se encuentra en condiciones de asumir la tarea que esta modalidad de combate le impone.

Por otro lado, puede darse la situación de que ese mando se halle al frente de un conflicto que podríamos considerar tradicional o convencional y en cuyo transcurso tenga a su alcance el desarrollo de operaciones cibernéticas. En este caso, la conclusión alcanzada no difiere de la anterior.

Tampoco aquí la novedad en cuanto a la modalidad de combate puede eludir la aplicación del DIH ni, por lo tanto, la responsabilidad del mando en cuanto a su debido cumplimiento. El hecho de que las ciberoperaciones sean lanzadas, en combinación con otros medios de guerra, hace que la aplicación del DIH quede reforzada y que la necesidad de adiestramiento se vislumbre como todavía más necesaria. Será precisamente esta la posibilidad en la que el mando de una operación se encuentre con mayor frecuencia. En ella deberá tener en cuenta las limitaciones que el DIH impone a todos los medios y métodos de combate y, por lo tanto, responderá del uso de estos en el caso de que él o sus subordinados cometan crímenes de guerra. De la misma forma que en el supuesto de ciberguerra, el mando deberá conocer las normas de DIH aplicables a estos métodos de combate e instruir convenientemente a sus subordinados.

Por último, del estudio de los ciberataques puede extraerse la conclusión de su potencial peligrosidad. No en vano, constituyen un poderoso medio de destrucción frente al que los Estados, en un momento dado, pueden llegar a dar una respuesta bélica. Si bien es cierto que la aplicación del DIH puede parecer a primera vista precipitada, no puede afirmarse que sea improcedente. Esto es así, una vez asumido que un ataque de esta índole entra dentro del concepto de ataque tal y como se define por el DIH. Por lo tanto, puede entenderse que la eventual respuesta bélica que al mismo se dé podrá desencadenar una ciberguerra u otro tipo de conflicto bélico, en el transcurso de los que serán de aplicación las limitaciones apuntadas.

Por lo tanto, cualquiera que sea la modalidad que revista un ataque cibernético, será posible la exigencia de responsabilidad al mando. Esta podrá originarse, bien directa, bien indirectamente, toda vez que el mando resulta responsable de los actos cometidos por sus subordinados, con independencia de que los haya ordenado directamente o no, ya que está obligado a conocer. Las normas convencionales y consuetudinarias que constituyen el DIH obligan al mando a identificar, prevenir o detener la comisión de un crimen de guerra y ello incluye, indefectiblemente, los realizados por medios cibernéticos.

Pero además, impone la adopción de la medida que resulte más eficaz para evitar esos crímenes. El adiestramiento, en este punto, resulta esencial. Examinada la materia que nos ocupa no puede más que concluirse que el hecho de contar con un nuevo método de combate supone la necesidad de adiestrar en el manejo de este, así como en las consecuencias que dicho uso puede originar. La formación en DIH ha de incluir las consecuencias que el uso del elemento cibernético puede tener desde el punto de vista del respeto a las normas de DIH.

El deber de saber que se impone a quien ejerza el mando de una operación se extiende al adiestramiento. Ello conlleva un ejercicio de reflexión futuro al objeto de extender analógicamente la labor desarrollada por los Tribunales Penales Internacionales, en su labor interpretadora en la determinación de la norma aplicable de DIH a la hora de exigir responsabilidad del superior por omisión, en el campo de las operaciones cibernéticas. Para que el adiestramiento recibido pueda considerarse adecuado y eficaz, al determinar la exigencia de esta responsabilidad por omisión, habrá que atender al conocimiento del nivel de suficiencia en el que es recibido por los subordinados. El recurso a los Asesores Jurídicos, por tanto, será esencial en numerosas ocasiones, en esa tarea de determinar el nivel de suficiencia.

Por otra parte, ha quedado expuesto que la ausencia de medidas preventivas necesarias y razonables no podrá ser compensada con medidas de sanción, por lo que puede concluirse que si la obligación de prevenir impuesta por el DIH implica necesariamente un eficaz adiestramiento, a su vez, la ausencia o inadecuación de este adiestramiento tendrá como resultado la posibilidad de exigir la correspondiente responsabilidad al mando.

Fuentes normativas y jurisprudenciales

Fuentes normativas

a) Nacionales

Código Penal y jurisprudencia, Aranzadi, 1.ª edición, Pamplona, 2013.

Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas *(BOE, n.º 33, de 7 de febrero de 2009).*

b) Internacionales

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 la mejora de la suerte de los heridos, enfermos y náufragos de las fuerzas armadas en el 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).*

Estatuto de la Corte Penal Internacional, aprobado en Roma el 17 de julio de 1998 y entrado en vigor el 1 de julio de 2002.

Estatuto del Tribunal Penal para la Antigua Yugoslavia, establecido mediante Resolución 827 (1993), adoptada por el Consejo de Seguridad en sesión de 25 de mayo de 1993.

Estatuto del Tribunal Penal para Ruanda, establecido mediante Resolución 955 (1994), adoptada por el Consejo de Seguridad en su sesión de 8 de noviembre de 1994.

Sentencias y decisiones judiciales

a) De tribunales de ordenamientos extranjeros

Corte Militar Canadiense, caso *Canadá vs. Kart Meyer,* veredicto del 28 de diciembre de 1945.

Corte Suprema de Estados Unidos, caso *Yamashita,* decisión de 4 de febrero de 1946.

b) De tribunales penales internacionales

Prosecutor vs. Delalic y otros (caso Celebici), caso IT-96-21-T, sentencia de 16 de noviembre de 1998.

Prosecutor vs. Dusko Tadic, Case nº IT-94-I-A, ICTY Appeals Chamber, Judgement 15 de julio de 1999.

Prosecutor v. Zoran Kupreskic and others, TPIY, Sala de primera instancia, caso n.º IT-95-16-T, sentencia de 14 de enero de 2000.

Prosecutor vs. Blaskic, caso IT-95-14T, sentencia de 3 de marzo de 2000.

Prosecutor vs. Bagilishema, caso ICTR-95-1-T, sentencia del 7 de junio de 2001

Prosecutor vs. Naser Oric, caso IT-03-68-T, Judgement, 30 de junio de 2006.

Prosecutor v. Sefer Halilovic, caso n.º IT-01-48-A, sentencia de 16 de octubre de 2007.

CIBERGUERRA Y DERECHO. EL *IUS AD BELLUM* Y EL *IUS IN BELLO* EN EL CIBERESPACIO

Jerónimo Domínguez Bascoy
Coronel auditor

SUMARIO