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

Jerónimo Domínguez Bascoy
Coronel auditor

SUMARIO

I. INTRODUCCIÓN. II. CIBERSEGURIDAD Y CIBERDEFENSA. III. CIBERATAQUES Y CIBERGUERRA. IV. DEBATES BÁSICOS EN TORNO A LA REGULACIÓN JURÍDICA DE LA CIBERGUERRA. 4.1. ¿DEBE ESTAR SOMETIDA LA CIBERGUERRA A LÍMITES JURÍDICOS? 4.2. ¿CUÁL DEBE SER EL ENFOQUE JURÍDICO PREDOMINANTE EN ORDEN A MANTENER LA SEGURIDAD EN EL CIBERESPACIO? V. EL *IUS AD BELLUM* EN EL CIBERESPACIO. 5.1. ASPECTOS BÁSICOS DEL *IUS AD BELLUM*. 5.2. CIBEROPERACIONES EQUIVALENTES A UN «USO DE LA FUERZA» PROHIBIDO POR EL ARTÍCULO 2(4) DE LA CARTA DE LAS NACIONES UNIDAS. 5.3. ¿CUÁNDO CONSTITUYE LA «CIBERFUERZA» UN «CIBERATAQUE ARMADO»? 5.4. CIBERATAQUES ARMADOS REALIZADOS POR ACTORES NO ESTATALES. 5.5. APLICACIÓN DE LOS REQUISITOS DE LA LEGÍTIMA DEFENSA A LA EJERCITADA FRENTE A CIBERATAQUES ARMADOS. 5.6. LEGÍTIMA DEFENSA COLECTIVA FRENTE A CIBERATAQUES ARMADOS. 5.7. ADOPCIÓN DE MEDIDAS POR EL CONSEJO DE SEGURIDAD ANTE CIBEROPERACIONES CONSTITUTIVAS DE AMENAZAS A LA PAZ, QUEBRANTAMIENTOS DE LA PAZ O ACTOS DE AGRESIÓN. VI. EL *IUS IN BELLO* EN EL CIBERESPACIO. 6.1. APLICABILIDAD DEL *IUS IN BELLO* A LAS CIBEROPERACIONES. 6.2. EL CONCEPTO DE «CIBERATAQUE» EN EL *IUS IN BELLO*. 6.3. EL «TARGETING» EN LA CIBERGUERRA: PERSONAS. LA PARTICIPACIÓN DIRECTA DE CIVILES EN LAS CIBERHOSTILIDADES. 6.4. EL «TARGETING» EN LA CIBERGUERRA: OBJETOS. REDES Y CIBERINFRAESTRUCTURAS DE «DOBLE USO». 6.5. CIBERGUERREROS. VII. CONCLUSIONES.

1. INTRODUCCIÓN

El de la ciberguerra es un tema que, de un tiempo a esta parte, acapara una buena parte de la agenda informativa. En los medios de comunicación, tanto nacionales como foráneos, sean generalistas o especializados, es cada vez más frecuente toparse con noticias, documentales o reportajes[1] sobre un fenómeno que, tal vez sea por lo atractivo del término, parece suscitar inevitablemente la atención de los ciudadanos de la aldea global.

La difusión del fenómeno en los medios ha venido, asimismo, acompañada, y muy a menudo precedida, por reflexiones más profundas que, bien limitadas específicamente a aquel, bien enmarcadas más generalmente en el tratamiento de la ciberseguridad o de la ciberdefensa, se han ido gestando en el seno de *think tanks* públicos y privados[2]. De entre este conjunto de reflexiones que la ciberguerra ha suscitado, no son pocas las que, particularmente en el ámbito anglosajón, han afrontado el estudio

---

[1] A título de mero ejemplo, y limitándonos a nuestro país, podemos citar el documental emitido el 4 de octubre de 2012 por TVE, dentro del programa *En portada,* sobre la «Amenaza Cyber» (vídeo disponible en http://www.rtve.es/alacarta/videos/en-portada/portada-amenaza-cyber/1543800/); el reportaje sobre «Ciberguerra fría» que en el programa *La hora de Asia* de Radio Exterior se emitió el 20 de febrero de 2013 (podcast disponible en http://www.rtve.es/alacarta/audios/la-hora-de-asia/hora-asia-ciberguerra-fria-20-02-13/1695365/); las diversas noticias aparecidas en la prensa diaria acerca de la actividad de la Unidad 61398 del Ejército de Liberación Popular chino, como la publicada en *El País* del día 19 de febrero de 2013 (http://internacional.elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html); o, ya en la prensa más especializada, el amplio reportaje que en su número 294 (abril 2013), bajo el título de «La guerra silenciosa», la *Revista Española de Defensa* dedica a la ciberguerra.

[2] En este punto, resultan de cita obligada en nuestro país el *Cuaderno de Estrategia* 149 (diciembre 2010) del IEEE sobre «Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio» (http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf), la monografía 126 (febrero 2012) del CESEDEN sobre «El ciberespacio. Nuevo escenario de confrontación» (http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf), o el documento titulado *La Ciberseguridad Nacional, un compromiso de todos,* publicado en junio de 2012 por el Spanish Cyber Security Institute (https://www.inteco.es/studyCategory/Seguridad/Observatorio/Biblioteca/ciberseguridad_SCSI).

Más específicamente centrados en la ciberguerra, y ya fuera de nuestro país, existen numerosos estudios, muchos de ellos disponibles en la red, de entre los que cabe destacar: el informe titulado *On Cyber Warfare* (http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf), publicado en noviembre de 2010 por la Chatam House, o el memorándum 117 del Institute for National Security Studies israelí, publicado en mayo de 2012 bajo el título *Cyber Warfare: Concepts and Strategic Trends* (http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=152953).

del tema desde un punto de vista jurídico. La aplicación en el ciberespacio tanto de las normas a que se sujeta el uso de la fuerza en las relaciones internacionales, como de aquellas que regulan los medios y métodos de combate en caso de conflicto armado, ha ido generando un ya amplio corpus doctrinal a partir del estudio pionero de Michael N. Schmitt del año 1999[3]. Ha sido, precisamente, este autor quien ha asumido la dirección de un grupo internacional de expertos que, con el patrocinio del NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE)[4], ha redactado el conocido como *Manual de Tallin sobre el Derecho Internacional aplicable a la Ciberguerra,* de reciente publicación[5], que constituye, sin duda, el mayor y más acabado esfuerzo realizado hasta el momento en el empeño de fijar un marco jurídico delimitador del uso de la fuerza en el ciberespacio.

Apenas nada es lo que, sin embargo, se ha publicado al respecto en nuestro país[6], donde el análisis jurídico de la ciberseguridad se ha centrado casi exclusivamente en el fenómeno de la ciberdelincuencia[7], siendo, en este sentido, el propósito de este trabajo el de sistematizar de manera esquemática, a efectos principalmente divulgativos, los principales debates jurídicos que se han producido hasta el momento en el ámbito doctrinal anglosajón. No se trata ahora, por tanto, de aportar enfoques novedosos, para lo cual ya habrá, en su caso, otras ocasiones en el futuro, a medida que los acontecimientos del mundo real nos vayan proporcionando nuevo material sobre el que reflexionar.

---

[3] Schmitt Michael, N., «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», en *Columbia Journal of Transnational Law,* vol. 37, 1998-1999, pp. 885-937. Disponible online en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800.

[4] https://www.ccdcoe.org/.

[5] *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, marzo de 2013.

[6] Quizás la única excepción sea el estudio de Ana Pilar Velázquez Ortiz, «Consideraciones sobre los ciberataques a la luz de los principios generales del empleo de las armas de conformidad con el Derecho Internacional Humanitario», comunicación presentada por la autora durante las IV Jornadas de Estudios de Seguridad que, bajo el título *Seguridad y conflictos: una perspectiva multidisciplinar,* celebró el Instituto Universitario General Gutiérrez Mellado durante los días 22, 23 y 24 de mayo de 2012. La comunicación se recoge en las pp. 435-463 de la obra que, con el mismo nombre de las jornadas, ha publicado el propio IUGM con las aportaciones más destacadas.

[7] La colaboración internacional en la lucha contra la ciberdelincuencia ya se ha plasmado en un convenio, elaborado en el seno del Consejo de Europa. Se trata del Convenio de Budapest sobre Ciberdelincuencia, hecho el 23 de noviembre de 2001 y ratificado por España por instrumento de 20 de mayo de 2010 *(BOE n.º 226, del 17 de septiembre de 2010).*

2. CIBERSEGURIDAD Y CIBERDEFENSA

Antes de afrontar el estudio jurídico del fenómeno de la ciberguerra, resulta conveniente situar conceptualmente el mismo dentro del marco general de la ciberseguridad y del más específico de la ciberdefensa.

Resulta ya axiomático señalar que la creciente ciberdependencia de las sociedades avanzadas lleva aparejada, como inevitable correlato, una también creciente cibervulnerabilidad. Son muchos los riesgos y amenazas, de distinto signo e intensidad, que, procedentes del ciberespacio, se ciernen sobre los distintos sectores gubernamentales, empresas privadas y ciudadanos cuyas actividades cotidianas se desarrollan cada vez en mayor medida en ese espacio virtual sin fronteras que, en su continua senda de progreso tecnológico, ha creado el ser humano por medio de infraestructuras, redes y sistemas de información y telecomunicaciones. Riesgos y amenazas que no se han quedado solo en eso, sino que ya se han hecho realidad con lo que, de modo genérico, se han dado en llamar «ciberataques», de los que un día sí y otro también se nos da cuenta en los medios de comunicación.

No es de extrañar, por tanto, que estados, entidades supranacionales, como la Unión Europea, y organizaciones internacionales de seguridad y defensa, como la OTAN, hayan ido adoptando en los últimos tiempos, dentro de sus respectivos ámbitos, iniciativas tendentes a garantizar la ciberseguridad, entendida esta como el «conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo sus infraestructuras tecnológicas, los servicios que prestan y la información que manejan»[8].

Se han ido formulando así diversas estrategias de ciberseguridad[9], en las que, como es lo propio, tras un análisis del problema que plantean los riesgos y amenazas para la seguridad en el ciberespacio, se fijan los principios sobre los que han de basarse las políticas que han de adoptarse para

[8] Esta es la definición que se formula en la Orden Ministerial 10/2013, de 19 de febrero *(Boletín Oficial del Ministerio de Defensa n.º 40, del 26.02.13),* por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Otras definiciones similares se contienen, por ejemplo, en la Estrategia francesa en materia de defensa y seguridad de los sistemas de información (2011): «état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accesibles»; o en la Estrategia de ciberseguridad australiana (2009): «measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means».

[9] En la página web del NATO CCDCOE, dentro de la sección de «links», pueden consultarse gran parte ellas.

hacer frente a aquellos, se marcan los objetivos a alcanzar, se trazan las consiguientes líneas de acción y se determinan los responsables de hacerlo.

En España ya contamos, desde hace relativamente poco tiempo, con una esa Estrategia de Ciberseguridad Nacional que se nos venía anunciando desde la Directiva de Defensa Nacional de 2012[10]. La Estrategia de Seguridad Nacional, aprobada por el Consejo de Ministros del 31 de mayo de 2013, incluye en su capítulo 3, entre los riesgos y amenazas para la Seguridad Nacional, como no podía ser de otra forma, a las ciberamenazas, señalando que «los ciberataques, ya sean en sus modalidades de ciberterrorismo, ciberdelito/cibercrimen, ciberespionaje o *hacktivismo,* se han convertido en un potente instrumento de agresión contra particulares e instituciones públicas y privadas». Y, su capítulo 4, en el que se trazan las líneas de acción estratégicas, incorpora, consiguientemente, las relacionadas con la ciberseguridad, entre las que ahora cabe destacar la primera de ellas, relativa al «incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas con apoyo en un marco jurídico operativo y eficaz». No es de extrañar, entonces, que entre esas Estrategias de segundo nivel cuya promoción, impulso y aprobación se atribuye al Consejo de Seguridad Nacional, la primera en aprobarse, el 5 de diciembre de 2013, fuera, junto con la de Seguridad Marítima Nacional, la de Ciberseguridad Nacional. En ella aparece ya, lógicamente, más detallada esa primera línea de acción estratégica relacionada con la ciberseguridad, mencionándose entre las medidas integrantes de la misma las de:

– Ampliar y mejorar permanentemente las capacidades de ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional, consolidándose la implantación del Mando Conjunto de Ciberdefensa y potenciándose su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés.

- Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

[10] Directiva de Defensa Nacional 2012, «Por una Defensa necesaria, por una Defensa responsable». En su apartado 4, en el que se marcan las directrices a seguir durante la legislatura, se señala expresamente que «se participará en el impulso de una gestión integral de la ciberseguridad, en el marco de los principios que se establezcan al efecto en la Estrategia de Ciberseguridad Nacional».

Por su parte, la Unión Europea cuenta desde el 7 de febrero del presente año con su propia estrategia de ciberseguridad, «un ciberespacio abierto, protegido y seguro», presentada conjuntamente por la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Entre las cinco prioridades y acciones estratégicas que en la misma se establecen, figura, como no podía ser de otra forma, la de desarrollar una política de ciberdefensa y de las correspondientes capacidades en el marco de la Política Común de Seguridad y Defensa (PCSD). Se destaca así, expresamente, que los esfuerzos de la Unión Europea en materia de ciberseguridad deben tener también una dimensión ciberdefensiva. En esta línea, el 25 de marzo de 2013, el Grupo Político-Militar remitió una nota al Comité Político y de Seguridad[11], invitándole a mostrar su acuerdo con las recomendaciones que en la misma se contienen acerca de los aspectos de la PCSD que afectan a la estrategia de ciberseguridad de la Unión Europea. Entre otras, dichas recomendaciones incluyen la de mejorar las capacidades de ciberdefensa de los Estados miembro, la de revisar y comprobar los mecanismos de alerta temprana y de respuesta a la vista de las nuevas ciberamenazas o la de continuar y reforzar la cooperación UE-OTAN en materia de ciberdefensa.

Volviendo a España, no podemos dejar de poner de relieve el hecho de que esas vulnerabilidades y amenazas que plantea el dominio ciberespacial, unidas al carácter crítico de la información que procesan los sistemas de información y telecomunicaciones, a su múltiple dependencia y a la complejidad técnica, cantidad y dispersión geográfica de sus infraestructuras, ha llevado a que, con el fin de dirigir y coordinar las acciones de nuestras Fuerzas Armadas en este ámbito, se haya creado, también en fechas recientes, el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, mediante la Orden Ministerial 10/2013, de 19 de febrero[12]. A los fines del presente trabajo, y dando un paso más en la tarea de acotar el objeto de nuestro estudio, los aspectos de esta Orden sobre los que debemos poner el foco son los siguientes:

[11] Documento 7847/13, «PMG recommendations on the CSDP aspects of the Cybersecurity Strategy of the European Union». Accesible en http://www.statewatch.org/news/2013/apr/eu-council-cybersecurity-pmg-opinion-7847-13.pdf.

[12] Esta Orden Ministerial es el indudable fruto de los trabajos que a lo largo de los dos últimos años se han venido desarrollando en el EMAD, que han plasmado sucesivamente en la «Visión del JEMAD de la ciberdefensa militar» (enero de 2011), el «Concepto de ciberdefensa militar» (julio de 2011) y el «Plan de acción para la obtención de la capacidad de ciberdefensa militar» (julio de 2012).

1.º El ámbito de actuación de este nuevo mando, delimitado por las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional.

2.º La definición que se formula de la ciberdefensa militar como el «conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control de las Fuerzas Armadas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos».

3.º La misión que se encomienda a este nuevo mando consistente en el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas que conforman su ámbito de actuación, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

4.º Y, en consonancia con esto último, el cometido que, entre otros, se le atribuye de «ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional».

Amenazas, agresiones y respuesta militar legítima y proporcionada. No hace falta ser muy sagaz para darse cuenta de que –o al menos intuir que– con estos términos y expresiones nos hemos situado ya de lleno en lo que constituye el objeto de nuestro trabajo: la ciberguerra y, más concretamente, los límites jurídicos dentro de los cuales la misma debe desenvolverse.

3. CIBERATAQUES Y CIBERGUERRA

Diversos autores, como es, por citar a un colega, el caso del capitán de fragata del JAG de la US Navy Todd C. Huntley[13], han puesto de manifiesto el uso abusivo que, con frecuencia, se hace de los términos «ciberguerra» y «ciberataque», para referirlos a todo tipo de actividades no autorizadas en el ciberespacio, con independencia de la naturaleza de la actividad

[13] Huntley, T. C., «Controlling the use of force in cyber space: the application of the law of armed conflict during a time of fundamental change in the nature of warfare», *The Naval Law Review,* vol. 60. Newport (2010). Accesible en http://www.jag.navy.mil/documents/navylawreview/NLRVolume60.pdf.

concreta de que se trate, de quién la realiza o de las consecuencias resultantes de la misma. Casos de denegación distribuida de servicio (DDoS), de robo o alteración de información, de cibervandalismo o de inserción de códigos maliciosos diseñados para dañar o destruir datos o sistemas, son generalmente etiquetados todos ellos como «ciberataques», e incluso como «ciberguerra», sin tener en cuenta si el resultado de tales actividades es la causación de muertes o lesiones, de destrucción o daños materiales, o, simplemente, la mera pérdida de información. Las intrusiones y otras actividades llevadas a cabo por empleados descontentos, *hackers* adolescentes o delincuentes se confunden así con las realizadas por terroristas o las conducidas por personal militar o de servicios de inteligencia extranjeros.

La clara delimitación, por tanto, de lo que han de considerarse «ciberataques» y «ciberguerra», en sentido estricto y riguroso, resulta absolutamente necesaria a la hora de desarrollar políticas y doctrinas sobre el uso de las capacidades para actuar en el ciberespacio. E igualmente precisa resulta para la tarea, no siempre fácil, de delinear las correspondientes competencias entre los sectores gubernamentales policial, militar y de inteligencia que, como ha puesto de relieve Ulf Häussler[14], en muchas naciones se ha ido desarrollando mediante un proceso de frenos y contrapesos, al modo de una separación de poderes en miniatura dentro del poder ejecutivo.

La práctica totalidad de los autores que, para abordar el estudio del tema desde el punto de vista jurídico, se han puesto a la tarea de llevar a cabo esa delimitación conceptual, lo han hecho basándose en las definiciones oficiales estadounidenses sobre las llamadas «Computer Network Operations», elaboradas en el contexto de las «Information Operations». Han partido, así, de la clásica distinción entre «Computer Network Defense» (CND), «Computer Network Exploitation» (CNE) y «Computer Network Attack» (CNA). Debe, sin embargo, tenerse en cuenta que en noviembre de 2010 la madurez de los desarrollos doctrinales en el campo de las ciberoperaciones llevó a que la Junta de Jefes de Estado Mayor de los Estados Unidos elaborara una nueva terminología conjunta para las operaciones en el ciberespacio[15] que, por una parte, alinea los conceptos clave de las ciberoperaciones con los términos y definiciones doctrinales utilizados en otros dominios operacionales conjuntos y, por otra, reemplaza las viejas

[14] Häussler, U., «Cyber security and defence from the perspective of articles 4 and 5 of the NATO treaty», en *International Cyber Security Legal and Policy Proceedings,* NATO CCD COE (diciembre 2010). Accesible en https://www.ccdcoe.org/245.html.

[15] Memorándum del Vice Chairman de la Joint Chiefs of Staff sobre la «Joint Terminology for Cyberspace Operations», al que se une como anexo un «Cyberspace Operations Lexicon».

definiciones que se habían formulado en el contexto de las «Information Operations».

En este nuevo léxico militar conjunto de los Estados Unidos ya encontramos definida la «Cyber Warfare» (CW) como «An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions».

Por su parte, el concepto de «Cyber attack» aparece como «a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions».

En cuanto a la «Cyber Defense», la misma es definida como «the integrated application of DoD or US Government cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend designated networks, protect critical missions, and enable US freedom of action».

Finalmente, las «enabling actions», que también se incluyen en el concepto de «Cyber Warfare», comprenderían, básicamente, el conjunto de actividades de lo que en este nuevo léxico se denomina «Cyber Operational Preparation of the Environment», el cual aparece referido a aquellas «non-intelligence enabling functions within cyberspace conducted to plan and prepare for potential follow-on military operations».

En España carecemos de una definición oficialmente sancionada de «ciberguerra». No obstante, tanto en el «Concepto de ciberdefensa militar» del EMAD como en el subsiguiente «Plan de acción para la obtención de la capacidad de ciberdefensa militar»[16], al señalarse las tres diferentes capacidades en que se desdobla la ciberdefensa militar, la de defensa, la de explotación y la de respuesta, al definirse esta última se señala que la misma está constituida por «el conjunto de sistemas, infraestructuras, personal y medios de apoyo logístico asentados sobre unos principios y procedimientos doctrinales para la ejecución y mantenimiento de acciones y actividades orientadas a la realización de ciberataques como defensa frente a amenazas y ataques», añadiéndose que «incluye actividades de perturbación, denegación de uso, degradación o destrucción de información, servicios o sistemas de información y comunicaciones de potenciales adversarios y agentes hostiles».

[16] Véase, *supra,* n. 14.

El concepto de «ciberataque» que se formula en la Orden Ministerial 10/2013 va, sin embargo, mucho más lejos, incluyendo actividades que caen notoriamente fuera del marco de las ciberhostilidades propiamente dichas. Y es que al ponerse principalmente el énfasis en el hecho de que se comprometa la disponibilidad, integridad y confidencialidad de la información (es decir, acciones dirigidas hacia la capa semántica del ciberespacio), se da incluso la consideración de ciberataques a los simples accesos no autorizados, a los cuales, en puridad, más que como ciberataques, habría que calificarlos como ciberincidentes.

Diversos autores han tratado, asimismo, de delimitar los conceptos de ciberguerra y ciberataque.

En el seminal artículo de Michael N. Schmitt[17], al utilizarse la terminología oficial militar de los Estados Unidos vigente en la época, no se menciona ni una sola vez el término ciberguerra y, en cuanto al de ciberataque, las pocas ocasiones en que aparece, lo hace como sinónimo de CNA, en cuanto modalidad ofensiva de las «Information Operations». La misma línea sigue, más de diez años después, Marco Roscini[18] quien, limitando su estudio a los CNA, se decanta por utilizar las expresiones de «ciberfuerza» y «ciberataques», a fin de mantener la coherencia con el lenguaje usado en el Derecho Internacional. Así, Roscini asocia el concepto de ciberataques al uso hostil de la ciberfuerza, sea en forma de un acto aislado, como el primer ataque de un conflicto armado, como un ataque en el contexto de un conflicto armado en curso o, finalmente, como una reacción frente a un ataque previo, convencional o cibernético. Por su parte, la ciberfuerza la refiere a las operaciones ejecutadas por un Estado contra otro Estado, tanto ofensivas como defensivas, por medio del uso de información residente en ordenadores individuales, en algunos ordenadores dentro de una red o en redes de información enteras, con el propósito de incapacitarlos o de producir daños extrínsecos al propio ordenador o red. Excluye, Roscini, de su definición de ciberfuerza los ataques físicos o cinéticos contra infraestructuras de información y comunicaciones, así como el ciberespionaje y la ciberpropaganda.

El intento más reciente y acabado que, entre la doctrina jurídica, se ha llevado a cabo para delimitar los conceptos de que se trata es, quizás, el realizado por Oona A. Hathaway y Rebecca Crootof[19]. Tras contraponer

[17] Véase, *supra,* n. 3.

[18] Roscini, M., «World Wide Warfare - *Jus ad bellum* and the Use of Cyber Force», *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, pp. 85-130.

[19] Hathaway, O. A. y Crootof, R., «The Law of Cyber-Attack», Faculty Scholarship Series, Paper 3852, 2012.

las concepciones estadounidense y de la Organización de Cooperación de Shanghái[20], las autoras proponen y defienden una definición estricta de «ciberataque» que, seguidamente, contrastan con los conceptos de «cibercrimen» y «ciberguerra». Señalan, así, que «un ciberataque consiste en cualquier acción destinada a debilitar el funcionamiento de una red o sistema de información y comunicaciones con una finalidad política o de seguridad nacional»[21]. Siguiendo a las citadas autoras, esta definición comprende, entre otros, estos principales aspectos:

1.º La conducta en que consiste el ciberataque debe ser activa: acciones ofensivas o de defensa activa, como es el caso de las contramedidas electrónicas.

2.º El objetivo del ciberataque debe ser el de debilitar o perturbar las funciones de una red o sistema. Frente a la definición formulada en el seno de la Organización de Cooperación de Shanghái, basada en los medios, se adopta el enfoque centrado en los objetivos del ataque, seguido en la doctrina militar de los Estados Unidos. Se señala que con una definición basada en los medios, que abarque cualquier actividad que haga uso de la cibertecnología, se corre el riesgo de extender el concepto de ciberguerra para reprimir o constreñir la libertad de expresión y la manifestación del disenso político *online*.

3.º De lo que se trata con los ciberataques es de debilitar el funcionamiento de una red o sistema. El mero ciberespionaje o ciberexplotación no constituiría, así, un ciberataque, en tanto no implica la alteración de las redes o sistemas de un modo que afecte a su capacidad presente o futura de funcionar. Para «debilitar o perturbar el funcionamiento» de una red o sistema un actor debe hacer algo más que limitarse a observar pasivamente o a copiar datos, por mucho que eso se haga de manera clandestina.

4.º En cuanto a la «finalidad política o de seguridad nacional», se trata del elemento de la definición que sirve para distinguir el ciberataque del cibercrimen. Cualquier acción agresiva realizada por un actor estatal en el dominio ciberespacial afecta necesariamente a la seguridad nacional y es,

[20] En un acuerdo entre los gobiernos de los Estados miembro de la OCS sobre cooperación en el ámbito de la seguridad de la información, adoptado en la 61.ª reunión plenaria (diciembre de 2008), se define la «information war» como «mass psychological brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party». Se refleja de esta forma una visión expansiva de los ciberataques, para incluir dentro del concepto el uso de la cibertecnología para socavar la estabilidad política.

[21] Traducción nuestra de «A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose».

por lo tanto, un ciberataque, alcance o no el nivel de ciberguerra. Asimismo, los cibercrímenes cometidos por actores no estatales con una finalidad política o de seguridad nacional merecen también la consideración de ciberataques. Las acciones que no se realicen con esa finalidad, tales como, por ejemplo, los fraudes por internet o los robos de identidad o de propiedad intelectual, al no satisfacer este elemento de la definición de ciberataque, constituirán meros cibercrímenes.

Los actos de ciberguerra reunirían siempre, según estas autoras, las condiciones precisas para ser considerados como ciberataques. Sin embargo, no todo ciberataque sería constitutivo de ciberguerra. Únicamente, aquellos ciberataques cuyos efectos fueran equivalentes a los de un «ataque armado» convencional y aquellos que tienen lugar en el contexto de un conflicto armado alcanzarían el nivel de ciberguerra. A partir de aquí, pasan a examinar tanto cuándo un ciberataque constituye un ataque armado conforme al *ius ad bellum,* pudiendo así ser considerado propiamente como ciberguerra, como la forma en que las normas que gobiernan la conducción de las hostilidades, conocidas como *ius in bello,* podrían ser aplicables a los ciberataques.

Por lo que se refiere a los trabajos que sobre la ciberguerra se han realizado fuera del ámbito jurídico, también en ellos, como es lógico, se ha tratado de delimitar conceptualmente aquella. Así, por ejemplo, en el memorándum del Institute for National Security Studies israelí[22] se señala que, dentro de las actividades de seguridad contra enemigos en el ciberespacio, es común distinguir entre tres áreas:

1.ª Penetración en los sistemas enemigos con un propósito de espionaje, lo que no se considera ciberguerra.

2.ª Modalidades de lo que podría denominarse *soft cyber warfare,* entre la que se incluirían tanto las actividades de guerra psicológica, propaganda y revelación de información secreta, con las que se persigue influir en la opinión y conducta del enemigo y de quienes le apoyan, como las sanciones internacionales, con las que se trata castigar a quien ha violado las reglas establecidas, con el fin de que modifique su conducta. Se resalta, en este sentido, lo atractivo que resulta el ciberespacio para realizar operaciones relativamente sencillas desde el punto de vista técnico y con un impacto significativo, tales como cerrar el paso a las comunicaciones con naciones extranjeras.

[22] Véase, *supra,* n. 2.

3.ª Ciberguerra, propiamente dicha, que abarcaría las actividades en el ciberespacio dirigidas directamente a causar daño o destrucción al enemigo, atacando tanto a sus propios sistemas como, a través de ellos, a otros objetivos en los dominios físicos.

El Manual de Tallin[23], pese a tener por objeto el Derecho Internacional aplicable a la ciberguerra, no formula ninguna definición de esta. El acotamiento conceptual de la misma hay que encontrarlo, por tanto, de manera implícita en el texto de la obra, si bien las claves básicas se nos dan en la parte introductoria, al tratar sobre el alcance *(scope)* del manual, donde, advirtiéndose de que el término «cyber warfare» se utiliza allí en un sentido puramente descriptivo, no normativo, se marcan los límites de las ciberactividades que son objeto del mismo. Se señala, así, que las ciberactividades que caen por debajo del nivel de «uso de la fuerza» (tal y como este término es entendido en el *ius ad bellum*), como la cibercriminalidad, no son tratadas en modo alguno en el manual. Y, en cuanto a las actividades de ciberinteligencia, las mismas son examinadas solo en la medida en que se relacionen con las nociones de «uso de la fuerza» y de «ataque armado», propias del *ius ad bellum,* o sean relevantes en el contexto de un conflicto armado regido por el *ius in bello*. En definitiva, se afirma, no se trata de un manual sobre «ciberseguridad», tal y como este término es comúnmente utilizado. El ciberespionaje, el robo de propiedad intelectual y otra amplia variedad de actividades criminales en el ciberespacio constituyen, en efecto, auténticas y muy serias amenazas para los estados, corporaciones e individuos, pero tales asuntos no son tratados en el manual por cuanto en la respuesta, nacional e internacional, frente a tales amenazas poco o ningún papel desempeñan ni el Derecho Internacional relativo al uso de la fuerza ni el propio de los conflictos armados.

Por otra parte, el *Manual de Tallin* se centra en las operaciones ciber-ciber en sentido estricto, como serían, por ejemplo, los ciberataques dirigidos contra sistemas que regulan el funcionamiento de infraestructuras críticas o contra sistemas de mando y control enemigos. Se excluye del mismo, por consiguiente, el tratamiento jurídico de las operaciones cinético-ciber, tales como un ataque aéreo contra un centro de cibercontrol, dado que las mismas no plantean ningún problema interpretativo en cuanto a la aplicación del tradicional Derecho de los conflictos armados.

[23] Véase, *supra,* n. 5.

4. DEBATES BÁSICOS EN TORNO A LA REGULACIÓN JURÍDICA DE LA CIBERGUERRA

4.1. ¿Debe estar sometida la ciberguerra a límites jurídicos?

En el número de mayo de 2012 de la revista de la American Bar Association se recoge un interesante intercambio de opiniones acerca de esta cuestión bajo el título de «What is the Role of Lawyers in Cyberwarfare?»[24]. Polemizan al respecto Stewart A. Baker[25] y Charles J. Dunlap Jr.[26] a partir de las afirmaciones que, desde planteamientos radicalmente realistas, realiza el primero de ellos acerca de que los juristas no ganan guerras y de que es probable que estemos a punto de averiguar si las pueden perder. Mantiene Baker que juristas en todos niveles gubernamentales han puesto tantísimas pegas legales en torno a la ciberguerra que han dejado a los militares en una situación de incapacidad para luchar, e incluso para planear, una guerra en el ciberespacio. En su opinión, imponer límites a la ciberguerra es algo nefasto. Citando las palabras del que fuera primer ministro británico en 1932, Stanley Baldwin, cuando, a propósito de la guerra aérea, manifestó que «" […] la única defensa es la ofensiva, lo que significa que tienes que matar más mujeres y niños más rápido que el enemigo si quieres salvar a los tuyos», Baker señala que, si ahora queremos defendernos de los horrores de la ciberguerra, precisamos primero afrontarlos con la franqueza de un Stanley Baldwin y luego encomendar a nuestros estrategas militares, no a nuestros juristas, la tarea de construir una estrategia de ciberguerra para el mundo en que vivimos, y no para aquel en el que nos gustaría vivir.

En su réplica, Dunlap comienza afirmando que la actuación al margen de la legalidad, la anarquía jurídica, no puede servir para ganar las guerras de América en el siglo XXI, pero sí, seguramente, para perderlas. Y así, dice, lo entienden claramente los profesionales de la milicia, incluyendo especialmente a los responsables de la conducción de ciberoperaciones, por mucho que, extrañamente, algunos civiles piensen de otra forma. Afirma Dunlap que los mandos militares ya han visto antes esa película de «sin límites legales», y no les ha hecho ninguna gracia. La dirección seguida

[24] http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/.

[25] Actualmente socio del despacho Steptoe & Johnson, en Washington D. C., anteriormente ha trabajado para el Departamento de Seguridad Interior y para la Agencia Nacional de Seguridad de los Estados Unidos.

[26] General de División retirado del JAG de la USAF, actualmente es profesor en la Duke University School of Law.

tras el 11-S, continúa, condujo a la adopción de técnicas de interrogatorio hoy generalmente etiquetadas como tortura, que, unidas a otras políticas, pusieron a las Fuerzas Armadas en el camino de Abu Ghraib, una catastrófica explosión de criminalidad calificada como una «clara derrota» por algún líder militar, como fue el caso de quien fuera Comandante de las fuerzas estadounidenses en Iraq, el teniente general Ricardo Sánchez. Los mandos militares, prosigue Dunlap, saben que atenerse a la ley es algo esencial para dominar en los conflictos del siglo XXI, saben que la ley ha impregnado la guerra tanto como cualquier otra actividad humana y conocen los peligros de ignorar su poder e influencia. Recuerda Dunlap las palabras de Michael Reisman y Chris T. Antoniou en su libro *The Laws of War*[27] acerca de que «en las democracias modernas, incluso un conflicto armado limitado requiere una importante base de apoyo popular», y que «ese apoyo puede verse erosionado o incluso perderse rápidamente, sin importar lo valioso que pueda ser el objetivo político, si la gente cree que la guerra se está conduciendo de una manera injusta, inhumana o inicua». Concluye Dunlap su réplica a Baker señalando que no cabe duda de que algunos «Rambos de sillón» encontrarán seductora la teoría de «olvida la ley» de este, pero que desde una perspectiva militar no hay cuestión en que atenerse a la ley no es solo lo correcto; es también la fórmula inteligente y pragmática que sirve para ganar guerras. Hacer otra cosa distinta nos llevaría, seguramente, a perder en lo que, en un reciente artículo, el propio Dunlap ha calificado como «Cyber Lawfare»[28].

La postura que oficialmente respalda el gobierno de los Estados Unidos es la segunda, es decir, la patrocinada por Dunlap. En su Estrategia para el Ciberespacio[29], se afirma que el desarrollo de normas para regular la conducta de los estados en el ciberespacio no requiere una reinvención del Derecho Internacional consuetudinario, ni tampoco convierte en obsoletas las normas internacionales existentes; normas internacionales ya duraderas que guían el comportamiento de los estados, tanto en tiempo de paz como de conflicto, también se aplican el ciberespacio. Con mayor detalle, el Asesor Jurídico del Departamento de Estado, Harold Koh, en una conferencia patrocinada por el USCYBERCOM, que tuvo lugar el 18 de

[27] Reisman, W. M. y Antoniou, Ch. T., *The Laws of War: a comprehensive collection of primary documents on international laws governing armed conflict,* Vintage Books, 1994.

[28] Dunlap Jr., Charles J. *Cyber Lawfare?,* (abril de 2013), Biblioteca Digital de la ISN del ETH de Zurich. Accesible en: http://www.isn.ethz.ch/isn/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=163103&tabid=1454266499&contextid774=163103&contextid775=163100.

[29] International Strategy for Cyberspace (mayo de 2011)

septiembre de 2012[30], se pronunció a este respecto, señalando, entre otras muchas cosas, que los principios del Derecho Internacional son aplicables en el ciberespacio, que este no es una zona «law-free» en la que cualquiera pueda conducir actividades hostiles sin reglas ni restricciones, que algunas ciberactividades pueden, en ciertas circunstancias, constituir usos de la fuerza en el sentido del art. 2(4) de la Carta de las Naciones Unidas y del Derecho Internacional consuetudinario, que el derecho a la legítima defensa, reconocido en el art. 51 de la Carta, puede desencadenarse frente a ciberactividades equivalentes a un ataque armado o a una amenaza del mismo y, en fin, que, en el contexto de un conflicto armado, el Derecho de los Conflictos Armados *(ius in bello)* resulta aplicable para regular el uso de ciberherramientas en las hostilidades, tal como lo hace con otras herramientas.

En el estudio pormenorizado que Michael N. Schmitt ha llevado a cabo de las palabras de Harold Koh, para contrastar sus opiniones con las que se reflejan en el *Manual de Tallin*[31], aquel pone de relieve la sorprendente coincidencia existente entre ambos, constituyendo incursiones iniciales en la procelosa labor de explorar la medida en que las vigentes normas del Derecho Internacional se aplicarán en el ciberespacio.

4.2. ¿Cuál debe ser el enfoque jurídico predominante en orden a mantener la seguridad en el ciberespacio?

En un muy comentado artículo, Thomas Rid[32], profesor en el King's College de Londres, mantiene que la ciberguerra nunca ha sucedido en el pasado, que tampoco se está desarrollando en el presente y que nunca tendrá lugar en el futuro. Para este autor, todos los ciberataques que responden a motivaciones políticas no son más que meras versiones sofisticadas de tres actividades que son tan antiguas como la guerra misma: el sabotaje, el espionaje y la subversión.

Muchos otros autores han puesto, asimismo, de manifiesto, la exageración de la amenaza realmente existente en que incurren algunos como,

[30] El texto de la conferencia pronunciada por Harold Koh, que lleva por título *International Law in Cyberspace,* está accesible en http://www.state.gov/s/l/releases/remarks/197924.htm.

[31] Schmitt, M. N., «International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed», *Harvard International Law Journal,* vol. 54 (diciembre de 2012).

[32] Rid, Th., «Cyber War Will Not Take Place», *Journal of Strategic Studies,* vol. 35, n.º 1 (febrero de 2012).

por ejemplo, el que fuera secretario de Defensa de los Estados Unidos hasta el pasado mes de febrero, Leon E. Panetta, cuando advierten sobre la posibilidad de un «cyber-Pearl Harbor»[33]. Baste citar, en esta línea crítica, el capítulo que, dentro de la publicación *Strategic Trends 2012* del Centre for Security Studies del ETH de Zurich, se dedica a «The militarisation of cyber security as a source of global tensions»[34]. Afirma su autora que, dado que los potencialmente devastadores efectos de los ciberataques son tan aterradores, la tentación es muy fuerte no solo para imaginar los peores escenarios posibles, sino también para darles a menudo demasiada importancia pese a la muy baja probabilidad de que se hagan realidad. La creciente atención hacia la ciberseguridad, señala, no debe llevar a militarizar más el ciberespacio por el temor a las cibercapacidades de otros estados. Lo que es más necesario en el actual debate, afirma, es un alejamiento del pensamiento basado en temores sobre el fin del mundo y un acercamiento hacia una más sensata valoración de la amenaza que tenga en cuenta el contexto estratégico.

Estas visiones son también compartidas por algunos de los autores que se aproximan al tema desde la perspectiva jurídica. Quizás, el más prominente ejemplo sea el de Mary Ellen O'Connell[35].

Pone de relieve esta autora cómo los ciberataques a Estonia en 2007 y los que en 2008 tuvieron lugar durante el conflicto entre Rusia y Georgia han influido indudablemente en el pensamiento que defiende la militarización de las soluciones a los problemas de seguridad en el ciberespacio. Asimismo, señala, el uso en 2010 del gusano Stuxnet, muy probablemente obra de los Estados Unidos e Israel, para detener el programa nuclear de Irán, revela un interés de los gobiernos en el desarrollo de ciberarmas. Escribe, así, O'Connell sobre la «invención» de un problema de ciberguerra, y el consiguiente desenfoque en el tratamiento jurídico de la ciberseguridad impulsado desde sus mismos orígenes por autores que son principalmente expertos en el Derecho Internacional que regula el uso de la fuerza,

---

[33] Véase la noticia del *New York Times* acerca del discurso pronunciado por Panetta en octubre de 2012: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

[34] Capítulo 5 (Myriam Dunn Cavelty) de *Strategic Trends 2012. Key Developments in Global Affairs,* publicado por el Center for Security Studies, ETH Zurich (2012). Accesible en http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012.pdf.

[35] O'Connell, M. E.., «Cyber Security without Cyber War», *Journal of Conflict & Security Law,* Oxford University Press (2012), vol. 17, n.º 2, pp. 187-209. Accesible en http://jcsl.oxfordjournals.org/content/17/2/187.full.pdf?keytype=ref%2520&ijkey=T6J6KDRCRcHM4Ao.

y que ha llevado a que sea esta la aproximación dominante hacia el tema, al menos en los Estados Unidos.

Entiende O'Connell que los autores que, como Michael Schmitt, Walter Grey Sharp o George Walker, afrontan la ciberseguridad en la forma de seguridad militar, lo hacen basándose en casos hipotéticos en lugar de en el mundo real de la ciberinseguridad. Los problemas del mundo real, dice, son el cibercrimen y el ciberespionaje. Y, pese a reconocer que el del STUXNET es también un ejemplo del mundo real que está más directamente vinculado con la categoría de la defensa militar, mantiene que Irán no sería capaz de reunir varias de las condiciones precisas para recurrir a la fuerza en legítima defensa en caso de tratar de responder a ese ciberataque.

Para O'Connell, el Derecho Internacional permite regular el ciberespacio como una esfera económica y de comunicaciones, así como utilizar medidas coercitivas para responder legítimamente a las ciberprovocaciones de todo tipo. En la esfera económica, las respuestas a las violaciones se conocen como «contramedidas», mientras en el campo del control de armamentos son conocidas como «sanciones». Además, señala O'Connell, varios tratados sobre control de armas, tales como el de No Proliferación Nuclear o la Convención sobre Armas Químicas, proporcionan al Consejo de Seguridad la posibilidad de adoptar medidas en caso de violación, pudiendo asimismo extrapolarse esta vía para impulsar el desarme en el ciberespacio, tal y como viene proponiéndose por Rusia, sin que por el momento los Estados Unidos se hayan mostrado proclives a seguir esa línea[36] y manifestar su preferencia por la vía de la cooperación policial internacional.

Frente a la opción de que el ciberespacio puede ser protegido mediante fuerza militar o la amenaza de la misma en forma análoga a la estrategia de disuasión de la Guerra Fría, O'Connell propone, en suma, virar hacia el ciberdesarme y a la pacífica protección del ciberespacio.

A nuestro juicio (no podemos ahora evitar dar nuestra opinión), estos planteamientos suponen cerrar los ojos a riesgos y amenazas muy presentes, para los que es necesario prepararse, por baja que pueda ser la probabilidad de que se hagan realidad. Como ha escrito Michel Baud, un oficial del Ejército de Tierra francés, en un artículo que responde al

[36] Markoff, J. y Kramer, A. E., «U.S. and Russia Differ on a Treaty for Cyberspace». *New York Times* del 27 de junio de 2009. Véase en http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all&_r=0.

antes citado de Thomas Rid[37], «La cyberguerre n'aura pas lieu, mais il faut s'y préparer»[38]. Según Baud, el término ciberguerra remite a una realidad concreta, que parece natural abordar desde un ángulo militar. Todos los conflictos recientes han visto la utilización de ciberarmas y, señala Baud, aunque la afirmación de Rid no es del todo errada, por cuanto la ciberguerra no tiene autonomía estratégica, es decir, no puede existir por sí misma, lo cierto es que la guerra tradicional es algo bien real y las ciberoperaciones pueden ser uno de sus medios de acción. Si bien no es necesario, dice, prever una ciberguerra autónoma, una línea de ciberoperaciones dentro de la planificación estratégica permitirá a los estados mayores militares actuar en el ciberespacio.

Por ello, sin perjuicio de que, en efecto, la consecución de una mayor ciberseguridad reclame actuar en los frentes del ciberdesarme o de la cooperación policial internacional, una actitud atenta a –tomando prestadas las palabras de Stewart A. Baker– este mundo en el que vivimos, y no a aquel en que nos gustaría hacerlo, no puede volver la espalda a esas ciberactividades más agresivas que conforman lo que hemos dado en llamar ciberguerra. Y, en consecuencia, desde el punto de vista jurídico, deviene absolutamente necesario determinar si (y en qué medida) las normas del Derecho Internacional que regulan el uso de la fuerza en las relaciones internacionales *(ius ad bellum)* resultan de aplicación en el ciberespacio, así como establecer la aplicabilidad del Derecho de los Conflictos Armados *(ius in bello)* a las ciberoperaciones conducidas en el contexto de un conflicto armado. Esto es lo que desde hace algo más de una década han venido haciendo esos juristas expertos en tales campos, a los que se refería O'Connell, en un esfuerzo meritorio que ha dado sus frutos en el *Manual de Tallin.* Y a ello vamos a dedicar los dos siguientes epígrafes del presente trabajo.

5. EL *IUS AD BELLUM* EN EL CIBERESPACIO

5.1. Aspectos básicos del *ius ad bellum*

Como se señala en el *Manual de Tallin,* la práctica estatal está dando todavía los primeros pasos para clarificar cómo se aplica a las ciberope-

[37] Vid. *supra,* nota 34.

[38] Baud, M., «La cyberguerre n'aura pas lieu, mais il faul s'y préparer», *Politique Étrangère,* 2/2012. Accesible en http://politique-etrangere.com/tag/cyberguerre/.

raciones el *ius ad bellum,* es decir, la parte del Derecho Internacional que regula el recurso a la fuerza por los estados como instrumento de su política nacional. En particular, se afirma, la carencia de definiciones acordadas, de criterios y de umbrales para la aplicación de las normas que integran ese bloque jurídico genera un considerable grado de incertidumbre cuando tratamos de aplicar aquellas a la rápidamente cambiante realidad de las ciberoperaciones.

Lógicamente, antes de continuar, lo primero que debemos hacer es determinar cuáles son las normas básicas de ese *ius ad bellum* de cuya aplicación a las ciberoperaciones se trata.

Dejando ahora de lado la referencia a los precedentes, partiremos para ello de la Carta de las Naciones Unidas, adoptada a la conclusión de la Segunda Guerra Mundial, en la que por vez primeraen la historia se prohíben tanto el uso de la fuerza como la amenaza del uso de la fuerza en las relaciones internacionales, dándose, por tanto, un paso más allá del estadio previo, en el que la prohibición afectaba, simplemente, al recurso a la guerra (Pacto Briand-Kellog de 1928). La norma básica del vigente *ius ad bellum* es la que se contiene en el art. 2(4) de la Carta, en el que se establece que «los miembros de la organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas».

De las diversas cuestiones interpretativas que plantea este precepto, la de mayor relevancia es la relativa a qué debe entenderse por «uso de la fuerza». No vamos ahora a entrar en detalle en los diversos argumentos utilizados por los tratadistas para defender conceptos diversos a ese respecto[39]. Nos limitaremos a recoger la síntesis de la posición dominante, realizada por Katharina Ziolkowski[40], quien señala que ese uso de la fuerza a que se refiere el art. 2(4) de la Carta debe quedar restringido a la «fuerza armada» y que, en esta línea, hay dos aspectos fundamentales a tener en cuenta: por un lado, que, de acuerdo con una interpretación histórica, sistemática y teleológica de la norma, el uso de la fuerza no incluye medidas de mera coerción, sea esta de naturaleza política o económica; por otro lado, que, sin embargo, el «uso de la fuerza» no está limitado al empleo de armamento militar, puesto que en 1986 el Tribunal Internacional de Justicia,

[39] Una explicación detallada puede encontrarse en el artículo de Marco Roscini citado en la nota 20.

[40] Ziolkowski, K..,*Ius ad bellum in Cyberspace – Some Thoughts on the »Schmitt Criteria« for Use of Force,* NATO CCD COE Publications, Tallinn, 2012.

en el caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América) ya tuvo ocasión de reconocer la posibilidad de usos indirectos de la fuerza armada, al calificar así actividades tales como las de «armar y entrenar a los *contras*»[41].

El *ius ad bellum,* tal y como aparece regulado en la Carta de las Naciones Unidas, se completa seguidamente con las dos excepciones que en la misma se prevén a esa regla general de prohibición de la amenaza o el uso de la fuerza: el ejercicio del derecho de legítima defensa individual o colectiva y las acciones coercitivas emprendidas por el Consejo de Seguridad en el marco del capítulo VII de aquella.

Con respecto a la primera, dispone el art. 51 de la Carta que «ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales».

Muy brevemente, los aspectos que, a los fines del presente trabajo, nos interesa destacar en la hermenéutica de este precepto son los siguientes:

1.º El alcance que deba darse a la expresión «ataque armado». En opinión del grupo de expertos que ha elaborado el *Manual de Tallin,* dicha expresión no es totalmente coincidente con la de «uso de la fuerza» (armada) del art. 2(4) de la Carta. Obviamente, todo ataque armado implica un uso de la fuerza; sin embargo, como puso de relieve el Tribunal Internacional de Justicia en el citado asunto de Nicaragua contra los Estados Unidos, no todo uso de la fuerza alcanza el nivel de ataque armado. Recuerda Nils Melzer[42] que, en el citado caso, el Tribunal Internacional de Justicia encontró necesario distinguir entre las más graves

[41] Por el contrario, el TIJ no consideró que las maniobras militares realizadas por los Estados Unidos cerca de la frontera de Nicaragua, o el suministro de fondos a los contras, equivalieran a un uso de la fuerza.

[42] Melzer, N., *Cyberwarfare and International Law,* United Nations Institute for Disarmament Research (UNIDIR) Resources, 2011. Accesible en http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

formas de uso de la fuerza (las que constituyen ataques armados) de otras formas menos graves, como, por ejemplo, un mero incidente fronterizo, distinción que debe atender a la «escala y efectos» de la fuerza empleada. Sin embargo, el Tribunal dejó inconcluso su razonamiento, de forma que todavía hoy reina cierta confusión a la hora de realizar esa distinción. Está claro, como se afirma en el *Manual de Tallin,* que cualquier uso de la fuerza que produce lesiones o muertes o daña o destruye propiedades satisfaría el requisito de la «escala y efectos», pero que, sin embargo, con respecto al caso de acciones que, sin resultar en lesiones, muertes, daños o destrucción, producen consecuencias negativas extensas, no hay todavía una opinión establecida.

2.º El ejercicio del derecho a la legítima defensa reconocido en el art. 51 de la Carta debe atenerse a los siguientes principios:

a) *Necesidad:* el uso de la fuerza debe ser objetivamente necesario para evitar o repeler un ataque armado.

b) *Proporcionalidad:* el daño causado por la acción realizada en legítima defensa debe ser el requerido por la gravedad del ataque armado que con dicha acción se trata de evitar o repeler.

c) *Inminencia:* la acción en legítima defensa no puede, desde un punto de vista temporal, llevarse a cabo antes de que resulte realmente necesaria para repeler o evitar un ataque armado, esto es, debe dirigirse contra un ataque inminente o en curso con el propósito de evitarlo o repelerlo.

d) *Inmediatez:* para evitar que constituya venganza, la respuesta al ataque armado debe tener una proximidad temporal con este, habiendo de producirse dentro del tiempo racionalmente necesario para la identificación del atacante y la preparación de la respuesta.

Por lo que se refiere a la segunda de las excepciones, es decir, a la acción impulsada, vía mandato o autorización, por el Consejo de Seguridad, establece el art. 39 de la Carta que «el Consejo de Seguridad determinará la existencia de toda amenaza a la paz, quebrantamiento de la paz o acto de agresión y hará recomendaciones o decidirá qué medidas serán tomadas de conformidad con los artículos 41 y 42 para mantener o restablecer la paz y la seguridad internacionales». Estos artículos se refieren, el primero, a las medidas que no implican el uso de la fuerza armada, y a las medidas de mantenimiento o restablecimiento de la paz y seguridad internacionales ejecutadas por fuerzas aéreas, navales o terrestres, el segundo.

5.2. Ciberoperaciones equivalentes a un «uso de la fuerza» prohibido por el art. 2(4) de la Carta de las Naciones Unidas

Como escribe Marco Roscini[43], aun aceptando que el art. 2(4) de la Carta solo prohibe la «fuerza armada», la cuestión es qué significa «armada» y si los ciberataques pueden ser considerados un uso de fuerza «armada». Remitiéndose a la definición del Black's Law Dictionary, recuerda que «armado» significa «equipado con un arma» o «que implica el uso de un arma». Pero, continúa, «casi todos los objetos pueden ser usados como armas si la intención del usuario es hostil».

El Tribunal Internacional de Justicia, al emitir en 1996 su opinión consultiva acerca de la legalidad de la amenaza o el empleo de armas nucleares, declaró que las referencias al uso de la fuerza que se contienen en los artículos 2(4), 41 y 42 de la Carta «no hacen referencia a ciertas armas específicas» y que «se aplican a cualquier uso de la fuerza, con independencia de las armas empleadas».

El uso de la «fuerza armada» prohibido por el *ius ad bellum* no debe, por tanto, entenderse limitado al empleo de armas cinéticas, químicas, biológicas o nucleares. De hecho, señala Nils Melzer[44], apenas existe controversia sobre que las ciberoperaciones caen dentro de la prohibición del art. 2(4) de la Carta en tanto sus efectos sean comparables a los que resultan del empleo de armas cinéticas, químicas, biológicas o nucleares. Esto incluiría, sin duda alguna, la realización de ciberoperaciones como herramienta ofensiva o defensiva diseñada para causar muertes o lesiones personales o para dañar o destruir objetos e infraestructuras, independientemente de si tales efectos implican daños físicos, funcionales o una combinación de ambos. Ejemplos comúnmente utilizados entre los autores que han escrito al respecto son los de ciberoperaciones que manipularan los sistemas informáticos que controlan ciertas infraestructuras críticas, provocando el colapso de una central nuclear, la apertura de las compuertas de una presa sobre un área densamente poblada o la desactivación del sistema de control del tráfico aéreo en un aeropuerto en medio de condiciones meteorológicas adversas.

Los problemas surgen, entonces, con la calificación de aquellas otras ciberoperaciones que no causan muertes, lesiones, daños o destrucción. De lo que se trataría en este caso es de identificar qué ciberoperaciones pueden considerarse equivalentes a otras acciones, cinéticas o no cinéticas, que la

[43] Véase, *supra, op. cit.,* en n. 20.
[44] Vid., *supra, op. cit,.* en n. 44.

comunidad internacional entendería implican un uso de la fuerza. Michael Schmitt, en su trabajo pionero de 1999[45], identificó un cierto número de factores, que el mismo autor ha vuelto a utilizar en un artículo más reciente[46], y que, no por casualidad –aunque en cierto modo reelaborados–, aparecen recogidos en el *Manual de Tallin,* los cuales, afirma, es probable que tengan influencia en las valoraciones de los estados acerca de si una ciberoperación concreta equivale a un uso de la fuerza. Tales factores, muy sumariamente explicados, son los siguientes:

– *Severidad:* consecuencias que entrañan daño físico para los individuos o propiedades equivalen por sí solas a un uso de la fuerza. Las que simplemente generan mero inconveniente o irritación, no. Entre ambos extremos, cuanto mayor sea la incidencia en intereses nacionales de carácter crítico, mayor será la probabilidad de que una ciberoperación sea calificada como un uso de la fuerza.

– *Inmediatez:* cuanto antes se manifiesten las consecuencias de una ciberoperación, menor será la posibilidad de que los estados busquen un acomodo pacífico a la disputa o de prevenir los efectos dañinos de aquella.

– *Carácter directo:* cuanto más directa sea la relación causal entre el acto inicial y sus consecuencias, más probable será que los estados consideren al actor responsable de una violación de la prohibición del uso de la fuerza.

– *Invasividad:* cuanto más seguro sea un sistema, mayor será la preocupación de que el mismo sea penetrado. No obstante, aunque altamente invasivo, el espionaje no constituye por sí solo un uso de la fuerza. Por ello, acciones como, por ejemplo, la desactivación de los mecanismos de ciberseguridad para controlar las pulsaciones de un teclado es muy poco probable que, pese a su invasividad, sean vistas como un uso de la fuerza.

– *Mensurabilidad de los efectos:* Cuanto más cuantificables sean las consecuencias, mayor será la probabilidad de que se estime que los intereses del Estado se han visto afectados. Así, una ciberoperación cuyas consecuencias pueden ser evaluadas en términos concretos es más probable que sea caracterizada como un uso de la fuerza que otra cuyos efectos son puramente subjetivos o más difíciles de medir.

---

[45] Vid. *supra,* op. cit. en nota 3.

[46] Schmitt, M. «Cyber Operations and the *Jus ad Bellum* Revisited» (2011). Villanova Law Review, 56, págs. 569-606.

– *Carácter militar:* la existencia de un nexo entre la ciberoperación en cuestión y la conducción de operaciones militares aumenta la probabilidad de que aquella sea considerada un uso de la fuerza.

– *Implicación del Estado:* cuanto más evidente y cercano sea el nexo entre un Estado y una ciberoperación, más probable será que otros estados caractericen esta como un uso de la fuerza por aquel Estado.

– *Presunta legalidad:* dado que las normas internacionales tienen generalmente un carácter prohibitivo, los actos que no están prohibidos están consecuentemente permitidos. Por ejemplo, el Derecho Internacional no prohíbe la propaganda, las operaciones psicológicas, el espionaje o la mera presión económica per se. Por ello, ciberoperaciones que caigan dentro de estas y otras similares categorías serían presuntamente legales, por lo que sería poco probable que fueran consideradas usos de la fuerza.

Sin perjuicio de su utilidad, debe señalarse que estos factores no son, sin embargo, aceptados acríticamente por la generalidad de la doctrina, existiendo autores que han puesto ciertos reparos a los mismos. Quizás, los análisis críticos más incisivos sean los realizados por Katharina Ziolkowski[47] y Andrew C. Foltz[48]. Este último examina a la luz de los «criterios de Schmitt» el ataque a las centrifugadoras de uranio de la central iraní de Natanz en 2010 mediante el gusano STUXNET, que se sirvió del software utilizado en los controladores lógicos programables fabricados por Siemens. Escribe Foltz que el análisis del caso conforme a dichos criterios sugiere que la mayor parte de los estados caracterizarían STUXNET como un uso de la fuerza, puesto que el gusano era altamente invasivo, produjo un daño físico severo, directo y mensurable, estaba falto de una clara presunción de legitimidad y, muy probablemente, contó con apoyo estatal. No obstante, Foltz detecta algunas deficiencias en el enfoque analítico de Schmitt para caracterizar a las ciberoperaciones. Su más significativa observación se relaciona con la premisa de Schmitt de que los estados se basarán principalmente en las normas existentes. Tal y como algunos comentaristas predijeron –y STUXNET ha puesto de manifiesto–, el art. 2(4) de la Carta ha demostrado ser un débil freno para ciberataques ofensivos. Ello se debe en parte a las dificultades relacionadas con la observación, la medición y la atribución de las ciberoperaciones. Y, lo que es más importante, ello refleja

[47] Vid, *supra, op. cit.,* en n. 42.

[48] Foltz, A. C. «Stuxnet, Schmitt Analysis, and the Cyber "Use of Force"« Debate», *Joint Force Quarterly,* n.º 67 (cuarto trimestre de 2012). Accesible en http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_schmitt_oct2012.pdf.

el hecho de que el Derecho Internacional no es estático y que los principios del *ius ad bellum* no son exclusivamente los recogidos en las Carta de las Naciones Unidas. Mientras las interpretaciones contemporáneas del art. 2(4) son el reflejo de la distribución de los instrumentos tradicionales de poder, esto es, la fortaleza política, militar y económica, la actual colección de cibercapacidades y vulnerabilidades no se corresponde con esa distribución. Y, en consecuencia, estados con cibercapacidades o vulnerabilidades significativas (con independencia de su fuerza política, militar o económica) van probablemente a considerar factores que van más allá del art. 2(4) a la hora de caracterizar la legalidad de las ciberoperaciones. Más aun, dado lo relativamente novedoso del ciberespacio, es también probable que diferentes estados sopesen sus riesgos y oportunidades estratégicas de manera distinta.

Tomando prestadas las palabras de Nils Melzer[49], podemos concluir este apartado constatando que, en general, no existe todavía un consenso en cuanto al umbral preciso a partir del cual las ciberoperaciones serían equivalentes a una amenaza o uso de la fuerza ilegales. Y la verdad es que las ciberoperaciones, a menudo situadas dentro de esa zona gris entre la fuerza armada tradicional y otras formas de coerción, sencillamente no fueron previstas por los redactores de la Carta de las Naciones Unidas y, hasta el momento, ni la práctica estatal ni la jurisprudencia internacional proporcionan criterios claros en relación con el umbral a partir del cual las ciberoperaciones que no causan muertes, lesiones o destrucción deben entenderse prohibidas conforme al art. 2(4).

5.3. ¿Cuándo constituye la «ciberfuerza» un «ciberataque armado»?

Conforme a lo establecido en el art. 51 de la Carta de las Naciones Unidas, ya examinado de forma somera, un Estado que sea víctima del uso de ciberfuerza estará facultado para actuar en legítima defensa solo en la medida en que tal uso de ciberfuerza pueda ser calificado como equivalente a un «ataque armado».

Lo primero que hay que determinar es, entonces, en qué medida el derecho a emplear la fuerza en legítima defensa se extiende más allá de los ataques armados de naturaleza cinética para comprender también los ejecutados por medio de ciberoperaciones. En este sentido, se ha señalado que, desde un punto de vista gramatical, la noción de «ataque armado»

[49] Vid *supra, op. cit.,* en n. 44.

implica necesariamente el uso de un arma. Ya hemos indicado anteriormente, sin embargo, que el Tribunal Internacional de Justicia, en su opinión consultiva acerca de la legalidad de la amenaza o el empleo de armas nucleares, declaró que las referencias al uso de la fuerza que se contienen en los artículos 2(4), 41 y 42 de la Carta «se aplican a cualquier uso de la fuerza, con independencia de las armas empleadas». De esta forma, está universalmente aceptado, como se dice en el *Manual de Tallin,* que los ataques químicos, biológicos y radiológicos de la escala y con los efectos requeridos constituyen ataques armados frente a los que cabría ejercitar la legítima defensa. Y esto es así, a pesar de su naturaleza no cinética, por razón de que las consecuencias de tales ataques pueden incluir sufrimientos graves o muertes. El mismo razonamiento se aplicaría, entonces, a las ciberoperaciones.

Donde el tema de la transposición al ciberespacio de la noción de ataque armado se muestra más turbio es en lo relativo a la determinación de la «escala y efectos» que debe tener una ciberoperación para justificar que frente a la misma se ejercite el derecho a la legítima defensa. Esquematizaremos a continuación la posición mayoritaria de la doctrina al respecto, siguiendo para ello a Nils Melzer[50]:

1.º Ninguna duda se plantea en aquellos casos en que una ciberoperación produce efectos destructivos equivalentes a los normalmente causados mediante el uso de armas cinéticas, químicas, biológicas o nucleares.

2.º A la vista, sin embargo, de las consecuencias, más disruptivas que destructivas, de la mayor parte de los ciberataques, no resulta completamente satisfactorio interpretar el criterio de la «escala y efectos» exclusivamente en términos de efectos equivalentes a destrucción física. El problema de este enfoque es que en ocasiones puede resultar demasiado restrictivo, dejando, por ejemplo, fuera de la noción de ciberataque armado a la incapacitación de toda la red nacional de energía.

3.º Con el fin de llegar a una adecuada interpretación del criterio de la «escala y efectos» en ausencia de muerte, lesiones, daños o destrucción, cabría hacer, entonces, referencia a las llamadas «infraestructuras críticas», cuya protección ha sido siempre una preocupación fundamental de los estados en sus discusiones acerca de la ciberseguridad. De esta forma, puede mantenerse que un ciberataque cuyos efectos es poco probable que entrañen destrucción física sería, no obstante, equivalente a un «ataque armado» si con el mismo se persiguiera incapacitar infraestructuras críticas dentro de la esfera de soberanía de otro Estado.

---

[50] Vid *supra, op. cit.*. en n. 44.

Por otra parte, como señala Michael N. Schmitt[51], el hecho de que las ciberoperaciones puedan acompañar a la acción militar convencional no tiene incidencia alguna sobre la naturaleza del ataque. Por ejemplo, los ciberataques que cabe dirigir contra los sistemas de mando y control o de defensa aérea del enemigo como elemento de una más amplia operación militar pueden ser respondidos mediante el uso de la fuerza, con independencia de que por sí solos constituyan o no un ataque armado.

Se dice en el *Manual de Tallin* que ningún ciberincidente internacional ha sido hasta el momento caracterizado públicamente y sin ambigüedades como un ataque armado. En particular, las ciberoperaciones contra Estonia en 2007, a las que de forma muy extendida se dio en calificar como «ciberguerra», no fueron, sin embargo, reconocidas ni por la propia Estonia ni por la comunidad internacional como un ataque armado. El grupo internacional de expertos redactor del manual coincide, por su parte, con este planteamiento, al considerar que el umbral de la «escala y efectos» no fue alcanzado en esa ocasión. Un caso que se acerca más es el del STUXNET, en el que, a la vista del daño causado en las centrifugadoras de uranio iraníes, algunos miembros del grupo de expertos sí son de la opinión de que esa ciberoperación superó el umbral del ataque armado (aun cuando el mismo pudiera justificarse con base en una legítima defensa anticipada).

5.4. Ciberataques armados realizados por actores no estatales

Dejando ahora de lado los ciberataques realizados por actores no estatales bajo la dirección de un Estado y que, por tanto, serían atribuibles a este, dedicaremos unas breves líneas a la cuestión de si los ciberataques realizados por actores no estatales que no actúan bajo la dirección de un Estado pueden llegar a ser considerados ataques armados a efectos del recurso a la fuerza en legítima defensa.

Como recuerda el *Manual de Tallin,* tanto el art. 51 de la Carta de las Naciones Unidas como las normas internacionales consuetudinarias relativas al derecho a la legítima defensa se han considerado tradicionalmente aplicables únicamente a los ataques armados realizados por un Estado contra otro Estado, encuadrándose la respuesta frente a actos violentos de actores no estatales dentro del paradigma policial/judicial. Es, sin embar-

[51] Vid. *supra, op. cit.,* en n. 48.

go, una realidad, tal y como ha señalado Sean Watts[52], que los actuales entornos de seguridad internacional y transnacional, conformados por un aumento dramático de la capacidad destructiva de actores no estatales violentos, está comenzando a sugerir con intensidad la posibilidad de dar a la legítima defensa un papel que vaya más allá de las interacciones entre estados. Aunque se esperaba que lo hiciera, en dos recientes resoluciones el Tribunal Internacional de Justicia[53] ha evitado entrar a considerar el tema de si es posible un ejercicio de legítima defensa por parte de los estados en el contexto de operaciones transnacionales contra actores no estatales.

Sin embargo, como señala el propio Watts, muchos ven en las resoluciones del Consejo de Seguridad y en la respuesta de la OTAN a los ataques terroristas del 11 de septiembre de 2001 argumentos en favor de esa posibilidad. La escala y efectos de tales ataques, que, sin duda, permiten estimar rebasado el umbral del ataque armado, llevaron a que tanto el Consejo de Seguridad, en sus Resoluciones 1368 y 1373, como la OTAN, que invocó por primera vez el art. 5 de su tratado constitutivo, explícitamente se remitieran al derecho a la legítima defensa.

La mayoría de los expertos que han tomado parte en la redacción del *Manual de Tallin* concluyen que la práctica estatal ha consagrado un derecho a la legítima defensa frente a ataques armados de actores no estatales, tales como grupos terroristas o rebeldes. En este sentido, consideran que, por ejemplo, una ciberoperación devastadora realizada por un grupo de terroristas desde un Estado contra una infraestructura crítica localizada en otro Estado sería constitutiva de un ataque armado de esos terroristas contra este Estado.

5.5. Aplicación de los requisitos de la legítima defensa a la ejercitada frente a ciberataques armados

Ya hemos visto, siquiera someramente, que el ejercicio del derecho a la legítima defensa reconocido en el art. 51 de la Carta de las Naciones Unidas debe atenerse a los principios de necesidad, proporcionalidad, inminencia e inmediatez.

El juego de estos principios en el ciberespacio determina, que:

---

[52] Watts, S., «Low-Intensity Computer Network Attack and Self-Defense», *International Legal Studies,* vol. 87, 2011, US Naval War College.

[53] Opinión consultiva sobre las consecuencias jurídicas de la construcción de un muro en territorio palestino ocupado (2004) y fallo en el caso de las actividades armadas en el territorio del Congo (2005).

1.º El uso de la fuerza no será legítimo en respuesta al daño ya producido como consecuencia de ciberoperaciones hostiles, siéndolo únicamente cuando de lo que se trate sea de evitar o repeler un ciberataque inminente o en curso.

2.º La necesidad de la fuerza empleada debe relacionarse con la existencia o inexistencia de medios de acción alternativos que no impliquen el uso de aquella. Si basta con la utilización de medios de ciberdefensa pasiva para frustrar un ciberataque armado, el uso de la fuerza debe descartarse. Por contra, cuando se prevé que medidas que no impliquen uso de la fuerza serán razonablemente insuficientes para frustrar el ciberataque o evitar otros posteriores, el derecho a la legítima defensa permitiría el uso de fuerza, fuera esta cinética o cibernética.

3.º La fuerza, cinética o cibernética, empleada debe ser proporcionada, lo que significa que la extensión y naturaleza de la respuesta debe limitarse a asegurar que el Estado víctima de un ciberataque armado no va a recibir nuevos ataques.

4.º La velocidad y el carácter impredecible y clandestino de la mayor parte de los ciberataques obstaculizan seriamente la capacidad del estado víctima para reaccionar a tiempo de detectar y evitar o repeler un ciberataque inminente o en curso. La ciberdefensa se basa en gran medida en sistemas automatizados, lo que determina que la verificación de la identidad del atacante y la valoración de la necesidad y proporcionalidad de la respuesta sean algo tremendamente difícil. Estas características de los ciberataques, unidas al hecho de que los mismos son cada vez en mayor medida realizados por actores no estatales, han dado lugar a que se haya extendido al ciberespacio el debate acerca de la permisibilidad de la legítima defensa anticipada. Dentro del grupo de expertos redactor del *Manual de Tallin* se manifestaron distintos enfoques sobre la cuestión, si bien la mayoría se decantó por el estándar de la «última ventana de oportunidad viable». Conforme al mismo, un Estado podría hacer uso de una legítima defensa anticipada contra un ataque armado, fuera cinético o cibernético, cuando, estando el atacante claramente decidido a lanzar el ataque, el Estado destinatario del mismo perdería su oportunidad de defenderse a menos de que actuara. Esta ventana de oportunidad puede presentarse inmediatamente antes del ataque en cuestión o, en algunos casos, después. Lo importante no es la proximidad temporal de la acción defensiva anticipada con el ataque armado futuro, sino si dejar de actuar en un momento dado llevaría razonablemente a esperar que el Estado atacado fuera incapaz de defenderse efectivamente en el momento en que el ataque comenzará realmente.

5.6. Legítima defensa colectiva frente a ciberataques armados

El art. 51 de la Carta de las Naciones Unidas permite tanto la legítima defensa individual como la colectiva frente a un ataque armado. En el *Manual de Tallin* no puede, por tanto, menos que reconocerse que ese derecho puede ejercitarse colectivamente, añadiéndose que la legítima defensa colectiva contra una ciberoperación equivalente a un ataque armado solo puede ser ejercida a solicitud del Estado víctima del ataque y dentro del alcance de la solicitud.

El recurso a la legítima defensa colectiva es objeto de tratados internacionales firmados al efecto, de los cuales el ejemplo señero, y que más de cerca nos toca, es el Tratado del Atlántico Norte, firmado en Washington el 4 de abril de 1949. Como es bien sabido, en su art. 5 dispone que:

> «Las Partes convienen en que un ataque armado contra una o contra varias de ellas, acaecido en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas y en consecuencia acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la parte o partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada para restablecer y mantener la seguridad en la región del Atlántico Norte. Todo ataque armado de esta naturaleza y toda medida adoptada en consecuencia se pondrán inmediatamente en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las medidas necesarias para restablecer y mantener la paz y la seguridad internacionales».

Por lo que respecta a la aplicación de esta previsión en el ciberespacio, baste señalar que en el Informe NATO 2020[54], elaborado en 2010 por un grupo de expertos presidido por Madeleine Albright, en el que se contienen análisis y recomendaciones para un nuevo concepto estratégico de la Alianza, dentro del capítulo 5, relativo a fuerzas y capacidades, al tratar de las capacidades de ciberdefensa se afirma que el siguiente ataque importante contra la Alianza bien podría venir a través de un cable de fibra óptica. Tras reconocerse que con frecuencia los sistemas de la OTAN son

[54] NATO 2020: ASSURED SECURITY; DYNAMIC ENGAGEMENT (17 de mayo de 2010). Accesible en http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf.

objeto de ciberataques que, muy a menudo, se producen por debajo del umbral de preocupación política, se añade que, sin embargo, el riesgo de un ataque a gran escala contra sus sistemas de mando y control o redes de energía podría justificar fácilmente la realización de consultas conforme al art. 4 del Tratado de Washington y, posiblemente, conducir a la adopción de medidas de defensa colectiva conforme al art. 5.

Ulf Häussler[55], al referirse a los ciberataques sufridos por Estonia en 2007, afirma que el análisis jurídico de los mismos lleva a concluir que, desde la perspectiva de la seguridad y defensa colectivas, estos ataques no rebasaron el nivel de una molestia importante y que, aunque el art. 4 del Tratado de Washington no fue expresamente invocado, el mecanismo de respuesta colectiva de la OTAN mostró su adecuada capacidad de reacción. De acuerdo con los informes disponibles, señala Häussler, tuvieron lugar consultas y las capacidades para permitir una valoración militar de la situación estuvieron disponibles.

5.7. Adopción de medidas por el Consejo de Seguridad ante ciberoperaciones constitutivas de amenazas a la paz, quebrantamientos de la paz o actos de agresión

Hemos visto que si, conforme a lo previsto en el art. 39 de la Carta de las Naciones Unidas, el Consejo de Seguridad determina la existencia de alguna de esas situaciones, podrá decidir la adopción de medidas que no impliquen el uso de la fuerza (art. 41) o, de estimar que las mismas pueden ser inadecuadas o han demostrado serlo, de las acciones de fuerza armada necesarias para mantener o restablecer la paz y la seguridad internacionales (art. 42).

Hasta la fecha, como dice el *Manual de Tallin,* el Consejo de Seguridad nunca ha determinado que una ciberoperación constituya una amenaza para la paz, un quebrantamiento de la paz o un acto de agresión. Pero, del mismo modo en que ya ha calificado como amenazas para la paz el terrorismo internacional (Res. 1373, de 2001) y la proliferación de armas de destrucción masiva (Res. 1540, de 2004), bien podría en un futuro hacer lo mismo con determinado tipo de ciberoperaciones, concretamente con las dirigidas contra infraestructuras críticas.

Entre las medidas que no implican hacer uso de la fuerza previstas en el art. 41 de la Carta se comprende la de interrupción total o parcial de las

[55] Vid. *supra, op. cit.,* en n. 16.

comunicaciones, lo que, lógicamente, puede extenderse a las cibercomunicaciones, para cuya aplicación será, entonces, preciso que los estados, en su ámbito doméstico, dispongan lo conveniente para que tal interrupción sea jurídicamente obligatoria para los proveedores de internet que operan dentro de su jurisdicción.

En cuanto a las medidas que implican el uso de la fuerza armada, previstas en el art. 42 de la Carta, en el *Manual de Tallin,* nada inocentemente, se pone el ejemplo de un Estado que desarrolla un programa de armamento nuclear, que ha ignorado las demandas del Consejo de Seguridad para poner fin a sus actividades y que se ha resistido a la sanciones económicas impuestas conforme al art. 41 de la Carta; caso en el cual el Consejo de Seguridad podría autorizar a los Estados miembros para que condujeran ciberoperaciones dirigidas a poner fin a la continuación de ese programa nuclear. El caso STUXNET, en definitiva.

Recuerda, no obstante, Michael N. Schmitt[56] que todo el sistema de seguridad colectiva de Naciones Unidas depende de la disposición de los cinco miembros permanentes del Consejo de Seguridad a posibilitar la acción absteniéndose de ejercitar su derecho de veto. Y, teniendo en cuenta la presencia en ese selecto grupo de Rusia y China, de cuyos territorios emanan regularmente las ciberoperaciones, cabe presumir que no será fácil que las Naciones Unidas emprendan una acción efectiva frente a aquellas ciberoperaciones que, de alguna manera, pudieran poner en peligro la estabilidad internacional.

6. EL *IUS IN BELLO* EN EL CIBERESPACIO

6.1. Aplicabilidad del *ius in bello* a las ciberoperaciones

El *ius in bello,* conocido generalmente como Derecho Internacional Humanitario (DIH) o Derecho de los Conflictos Armados y, más antiguamente, como Derecho de la Guerra, se concibe en la actualidad, tal y como señala Manuel Pérez González[57], «como un vasto conjunto normativo que persigue controlar jurídicamente el fenómeno bélico –reglamentando los métodos y medios de combate, distinguiendo entre personas y bienes ci-

[56] Vid *supra, op. cit.,* en n. 48.

[57] Pérez González, M., «El Derecho Internacional Humanitario frente a la violencia bélica: una apuesta por la humanidad en situaciones de conflicto», en *Derecho Internacional Humanitario,* Centro de Estudios de Derecho Internacional Humanitario de Cruz Roja Española, Tirant lo Blanch, 2007.

viles y objetivos militares, protegiendo a las víctimas y a quienes las asisten–, con vistas a limitar en la mayor medida posible los ingentes males que el mismo causa a los seres humanos».

De manera muy sintética, recordaremos que las fuentes más importantes del DIH están constituidas por los cuatro Convenios de Ginebra de 12 de agosto de 1949[58], sus dos Protocolos Adicionales de 8 de junio de 1977[59], además de por el conocido como Derecho de La Haya, ciudad en las que se celebraron las Conferencias de la Paz de 1899 y 1907, en la segunda de las cuales se aprobaron catorce convenios, de los cuales el de mayor interés a nuestros efectos es el número IV, que lleva anejo el Reglamento sobre las leyes y costumbres de la guerra terrestre. Hay que tener en cuenta también que, además de estas normas convencionales, existe un *ius in bello* consuetudinario, que ha sido objeto de un laborioso estudio publicado por el Comité Internacional de la Cruz Roja[60], en el que se comprenden aquellas normas del DIH que, por ser parte del Derecho Internacional consuetudinario, resultan de aplicación a cualquier parte en un conflicto armado, independientemente de que haya ratificado o no los tratados en que se contienen las mismas reglas u otras similares.

La cuestión que se plantea, entonces, es si este *ius in bello* (al que en lo sucesivo nos referiremos como DIH) resulta aplicable –y, en su caso, cómo se aplicaría– a lo que podemos denominar «ciberhostilidades».

La tesis mayoritariamente compartida, que es la que refleja el *Manual de Tallin,* es la de que las ciberoperaciones ejecutadas «en el contexto de un conflicto armado» se encuentran sujetas a las normas del DIH. No obstante, los miembros del grupo de expertos se hallan divididos en lo que respecta a la naturaleza del nexo entre la ciberoperación y el conflicto armado: para unos, el DIH se aplicaría a cualquier tipo de ciberactividad conducida por una parte en un conflicto armado contra su oponente, mientras que, para otros, para que ello fuera así esa ciberactividad debería ser realizada en ejecución de las hostilidades, como contribución al esfuerzo militar. Así, se pone el ejemplo de una ciberoperación lanzada durante un conflicto

[58] I Convenio: para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña; II Convenio: para aliviar la suerte que corren los heridos, los enfermos y los náufragos de las fuerzas armadas en la mar; III Convenio: relativo al trato debido a los prisioneros de guerra; IV Convenio: relativo a la protección debida a las personas civiles en tiempo de guerra.

[59] Protocolo I: relativo a la protección de las víctimas de los conflictos armados internacionales; Protocolo II: referente a la protección de las víctimas de los conflictos armados sin carácter internacional.

[60] Henckaerts, J.-M., *Study on customary international humanitarian law: a contribution to the understanding and respect for the rule of law in armed conflict,* 2005.

armado desde el Ministerio de Comercio de un Estado contra una corporación privada de un Estado enemigo con el fin de hacerse con secretos comerciales, que para los primeros estaría sujeta al DIH, mientras que para los segundos no.

Se pregunta, por otra parte, Nils Melzer[61], si (y en qué circunstancias) pueden las ciberoperaciones ser desencadenantes de un conflicto armado, esto es, si las ciberoperaciones pueden constituir por sí mismas un conflicto armado sin que paralelamente tengan lugar hostilidades convencionales. O, lo que es lo mismo, si las ciberhostilidades pueden determinar por sí solas que se aplique el DIH. La respuesta que el propio Melzer da a la pregunta que se autoplantea es afirmativa en la medida en que esas ciberhostilidades reúnan los elementos constitutivos de un conflicto armado, sea este internacional o no internacional.

En el caso de un conflicto armado internacional, las ciberoperaciones deberían entrañar el «recurso a la fuerza armada entre dos o más estados». Lo que significa que las ciberoperaciones conducidas por un Estado o bajo su patrocinio darán lugar a un conflicto armado internacional siempre que vayan dirigidas a infligir daño a otro Estado, no solo mediante la causación de muerte, lesiones o destrucción, sino también afectando de modo adverso a sus operaciones o a su capacidad militar.

En el caso de un conflicto armado de carácter no internacional, son elementos constitutivos del mismo, por un lado, que exista, al menos, un beligerante no estatal que tenga un mínimo grado de organización y, por otro lado, que las confrontaciones armadas muestren un cierto nivel de intensidad. El primer criterio requiere una acción colectiva organizada, lo que con toda seguridad excluiría de la noción de conflicto armado a las ciberoperaciones conducidas por hackers individuales. Por otra parte, en tanto las ciberoperaciones emanen del territorio controlado por el Estado atacado, y siempre que no vayan acompañadas de la amenaza o el uso de fuerza militar convencional que pudiera impedir que el Estado ejerciera su autoridad territorial, tales ciberoperaciones serían probablemente consideradas en la práctica como un acto criminal frente al que se respondería con medidas de carácter policial/judicial.

En cualquier caso, una vez que se ha determinado la existencia de un conflicto armado, habrá que establecer la medida en que las reglas y conceptos tradicionales del DIH pueden transponerse a las ciberoperaciones conducidas en el contexto de ese conflicto. Eso es lo que trataremos de hacer a continuación, no sin antes resaltar, como lo hacen tanto el *Manual*

[61] Vid *supra, op. cit.,* en n. 44.

de Tallin como Erki Kodar[62], el hecho de que, en ausencia de normas explícitas que puedan ser de aplicación a las ciberoperaciones, la libertad de acción siempre estará limitada por la llamada «Cláusula Martens», recogida, entre otros, en el Protocolo Adicional I[63] en los siguientes términos: «En los casos no previstos en el presente Protocolo o en otros acuerdos internacionales, las personas civiles y los combatientes quedan bajo la protección y el imperio de los principios del derecho de gentes derivados de los usos establecidos, de los principios de humanidad y de los dictados de la conciencia pública».

Lo que significa que, siempre que se conduzcan ciberactividades en el curso de un conflicto armado, la «Cláusula Martens» servirá para asegurar que tales actividades no se llevan a cabo en un vacío legal.

6.2. El concepto de «ciberataque» en el *ius in bello*

No todas las ciberactividades que tienen la capacidad de mejorar la posición militar de quien hace uso de las mismas equivalen a «ataques» en el sentido que este término tiene en el DIH. Por tal razón, determinar qué es y qué no es un ciberataque es la tarea primordial que ahora tenemos que afrontar, pues de ella depende la aplicación a las ciberoperaciones de las muy numerosas normas del DIH que regulan, limitándolos, los ataques.

El principio de distinción, básico en el DIH, se formula en el art. 48 del Protocolo Adicional I, estableciéndose que «a fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares».

Es indudable que este principio es plenamente aplicable a las ciberoperaciones que se conducen durante un conflicto armado. Pero ¿a qué ciberoperaciones? A primera vista, podría pensarse, como dice Michael N. Schmitt[64], que el término «operaciones» que emplea el art. 48 del PA I de-

[62] Kodar, E., «Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I», *ENDC Proceedings,* vol. 15, 2012, pp. 107-132. Accesible en http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf.

[63] PA I, Artículo 1.2.

[64] Schmitt, M. N., «Cyber Operations and the Jus in Bello: Key Issues», en *International Law Studies,* vol. 87, 2011, US Naval War College. Accesible en http://www.usnwc.edu/Research---Gaming/International-Law/New-International-Law-Studies-(Blue-Book)-Series/International-Law-Blue-Book-Articles.aspx?Volume=87.

terminaría que quedara prohibida cualquier ciberactividad dirigida contra personas u objetos civiles. La lectura de los artículos siguientes pone de manifiesto, sin embargo, que el tipo de operaciones a las que se aplica ese principio de distinción es el constituido por los «ataques», de forma que operaciones que no tienen tal carácter (como podría ser el caso de las operaciones psicológicas, siempre que no causen daño físico ni sufrimiento humano) se consideran lícitas conforme al DIH.

En cuanto a qué es, exactamente, lo que debe entenderse por «ataques», establece el art. 49 del PA I que estos son «los actos de violencia contra el adversario, sean ofensivos o defensivos».

Lo que con William H. Boothby[65] cabe preguntarse seguidamente es cómo puede aplicarse la noción de «actos de violencia» en el contexto ciberespacial cuando para el lanzamiento de un ciberataque basta generalmente con hacer «click» con el ratón del ordenador o con pulsar la tecla «enter».

La ausencia de un impacto violento cinético no impide, sin embargo, según la práctica totalidad de los autores, que, siempre que se causen daños físicos equivalentes a los producidos con munición cinética mediante una ciberoperación, esta sea considerada como un «ciberataque» a los efectos de aplicación del DIH. Se dice, así, en el *Manual de Tallin,* que «a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects». Y se pone como ejemplo el de una ciberoperación que alterara el funcionamiento del sistema SCADA[66] de una red eléctrica provocando un grave incendio, cuyas consecuencias destructivas determinarían la consideración de aquella como ataque.

Existe, no obstante, desacuerdo en la doctrina acerca de si la noción de ataque incluye a aquellas ciberoperaciones cuya finalidad no es destruir, sino meramente, neutralizar el objetivo. Se suele citar a Knut Dörmann[67] como el principal exponente de este punto de vista, que basa en la definición de objetivos militares del art. 52.2 del PA I, en el que se incluyen, entre otros, aquellos objetos cuya «captura o neutralización» ofrezca en las

---

[65] Boothby, W. H., «The Law of Targeting», Oxford University Press, 2012, cap. 18.

[66] Acrónimo de «Supervisory Control And Data Adquisition», se refiere a un sistema informático que permite controlar y supervisar a distancia los procesos de infraestructuras industriales.

[67] Dörmann, K., «The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint» en Byström K. (ed.), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law,* 17-19 de noviembre de 2004, Estocolmo. Accesible en http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.

circunstancias del caso una ventaja militar definida. Otros autores entienden, por el contrario, que la interpretación literal de la expresión «actos de violencia» utilizada por el PA I para definir a los ataques requiere que, si no el acto en sí mismo, sí al menos sus consecuencias sean violentas. Citan estos últimos en apoyo de su tesis que el principio de proporcionalidad, tal y como se recoge en los art. 51.5. b) y 57.2.a) y b) del PA I, se formula con referencia a ataques que causen «muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas».

Para Nils Melzer[68], aunque ambas posiciones tienen sus puntos fuertes, ninguna parece proporcionar una interpretación enteramente satisfactoria de la noción de ataque en relación con las ciberoperaciones. Por una parte, dice, sería escasamente convincente excluir de la noción de ataque la incapacitación no destructiva del sistema de defensa aérea u otras infraestructuras críticas de carácter militar de un Estado, simplemente porque no causa directamente muerte, lesiones o destrucción. Pero, por otro, añade, sería bastante exagerado extender la noción de ataque a cualquier ciberoperación de denegación de servicio dirigida, por ejemplo, contra servicios de compra *online,* agencias de viaje o directorios telefónicos.

En el *Manual de Tallin* se recoge esta polémica, señalándose que entre el grupo de expertos hubo una gran discusión acerca de si la ciberinterferencia con la funcionalidad de un objeto constituye daño o destrucción. La mayoría mostraron la opinión de que esa interferencia es un daño si la restauración de la funcionalidad requiere la sustitución de componentes físicos, aunque hubo división de opiniones acerca de si el requisito del daño se entiende también cumplido cuando la funcionalidad del objeto puede restaurarse mediante una reinstalación de su sistema operativo. Algunos expertos fueron todavía algo más lejos, sugiriendo que la interferencia con la funcionalidad de un objeto que hace precisa, simplemente, una restauración de los datos, sin requerir la sustitución de componentes físicos o la reinstalación del sistema operativo, también debe ser considerada como un ataque, al entender aquellos que con la pérdida de utilidad del objeto se cumple el requisito del daño.

Finalmente, debe repararse asimismo en que, como también recuerda el *Manual de Tallin,* las ciberoperaciones pueden ser parte integrante de una más amplia operación constitutiva de un ataque. Así, por ejemplo, una ciberoperación dirigida a incapacitar el sistema de defensa de un objetivo que es luego atacado cinéticamente. El DIH se aplicaría, entonces, plenamente a tal tipo de ciberoperaciones.

---

[68] Vid *supra, op. cit.,* en n. 44.

6.3. El «targeting» en la ciberguerra: personas. La participación directa de civiles en las ciberhostilidades

Es un lugar común referirse al principio de distinción, que, como hemos visto anteriormente, se formula en el art. 48 del PA I, como uno de los principios básicos del DIH. Conforme a este principio, las operaciones militares solo pueden dirigirse únicamente contra determinadas personas u objetos: combatientes, miembros de grupos armados organizados, civiles que participan directamente en las hostilidades y objetivos militares.

El principio de distinción se traduce, así, en primer lugar, en la prohibición de dirigir ciberataques contra la población civil como tal o contra personas civiles individuales.

Existen, sin embargo, como también hemos apuntado, ciertas operaciones dirigidas contra la población civil que son lícitas, como la propaganda o las operaciones psicológicas. Por eso, las ciberoperaciones dirigidas a influir en los pensamientos de la población civil no estarían prohibidas siempre y cuando, por ejemplo, no se tratase de amenazas de violencia cuya finalidad principal fuera aterrorizar a la población civil, que estarían prohibidas por el art. 51.2 del PA I.

La protección de las personas civiles frente a los ataques se extiende hasta tanto tomen parte directa en las hostilidades y por el tiempo en que lo hagan. La noción de «participación directa en las hostilidades» parte del hecho de que en las guerras actuales la distinción entre combatientes y civiles, sobre cuya base descansa en gran medida el DIH, es a menudo difícil de mantener. La fórmula se introdujo en el PA I, cuyo art. 51.3 dice escuetamente que «las personas civiles gozarán de la protección que confiere esta Sección, salvo si participan directamente en las hostilidades y mientras dure tal participación».

La clarificación de la noción ha llevado a la publicación por el Comité Internacional de la Cruz Roja de una guía interpretativa[69], redactada por Nils Melzer a la vista de las conclusiones a que llegaron los componentes de un grupo de expertos que trabajaron en el tema entre 2003 y 2008. Como ha señalado David Turns[70], aunque la guía no se escribió específicamente con la ciberguerra en mente, sino que trata de elaborar la noción de «participación directa en las hostilidades» en general, hay en

[69] *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law,* International Committee of the Red Cross, 2009. Accesible en http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf.

[70] Turns, D., «Cyber Warfare and the Notion of Direct Participation in Hostilities», en *Journal of Conflict & Securiry Law,* vol. 17, n.º 2, 2012, pp. 279-297.

ella algunos pasajes que tienen directa relación con la situación de civiles participando directamente en ciberhostilidades. No es, por tanto, extraño que en el *Manual de Tallin* se dedique a la cuestión una atención detallada. Los miembros del grupo de expertos estuvieron en general de acuerdo con los tres criterios acumulativos que, para la calificación de un acto como participación directa en las hostilidades, se exigen en la guía:

1.º El acto debe tener el efecto, pretendido o real, de afectar negativamente a las operaciones o capacidades militares del adversario, o infligir muerte, daños físicos o destrucción material de personas u objetos protegidos contra ataques directos (umbral de daño). De esta forma, actos que sin llegar a constituir ciberataques afectaran negativamente al enemigo desde el punto de vista militar satisfarían este criterio. Por ejemplo, una ciberoperación que desbaratara el sistema de mando y control del enemigo.

2.º Debe existir una relación de causalidad entre el acto en cuestión y el daño infligido o pretendido (nexo causal).

3.º El acto debe estar directamente relacionado con las hostilidades (nexo de beligerancia).

Por otra parte, dos cuestiones debatidas entre los participantes en la elaboración del manual que, en relación con este tema, merecen mencionarse son, en primer lugar, la relativa a las ciberoperaciones de «efectos retardados». Así, por ejemplo, el emplazamiento de una bomba lógica diseñada para activarse en un momento futuro. La mayor parte de los expertos adoptaron la posición de estimar que la duración de la participación directa en las ciberhostilidades se extendería desde el momento de la implicación del individuo en el planeamiento de la misión hasta el momento en que dejara de tener un rol activo en la misma, que no tendría necesariamente que corresponderse con el momento en que se produjera el daño. Piénsese en el caso de una bomba lógica emplazada por una persona y activada por otra distinta.

En segundo lugar, otra cuestión debatida, relacionada con la duración de la participación directa en las hostilidades, y, por tanto, con la susceptibilidad de ser atacado, es la relativa a aquella situación en la que un individuo lanza repetidas ciberoperaciones cada una de las cuales constituye un acto de dicha participación directa. Imaginemos, continúa el manual, a un «hacktivista» individual que, en el curso de un mes, conduce siete ataques contra el sistema de mando y control del enemigo. Para unos expertos, únicamente sería susceptible de ataque mientras estuviera conduciendo cada uno de esos ataques concretos. Para otros, esta interpretación daría lugar a

esa situación que, en una metáfora ya clásica, se conoce como «puerta giratoria» *(revolving door),* carente de sentido desde el punto de vista operacional, por lo que ese «hacktivista», entienden, sería susceptible de ataque, como participante directo en las hostilidades, durante el mes completo a lo largo del cual realizó sus ataques.

6.4. El «targeting» en la ciberguerra: objetos. Redes y ciberinfraestructuras de «doble uso»

Establece el art. 52.2 del PA I que «los ataques se limitarán estrictamente a los objetivos militares» y que «en lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida».

Los ordenadores, redes de información y las ciberinfraestructuras pueden constituir objetivos militares y, en tal sentido, ser susceptibles de ataques. La mayoría de los expertos que tomaron parte en la elaboración del *Manual de Tallin* convinieron en que la noción de «objeto» del DIH no debe ser interpretada en el sentido de incluir los datos, dado su carácter intangible, aunque, sin embargo, una ciberoperación dirigida contra datos podría eventualmente ser considerada como un ataque en el caso de afectar a la funcionalidad de un ordenador o sistema. Una minoría de expertos opinó, por el contrario, que, a los fines del «targeting», los datos por sí mismos deben ser considerados como un objeto. En su opinión, no hacerlo así implicaría que incluso el borrado de muy valiosos conjuntos de datos civiles escaparía potencialmente a la regulación del DIH, contradiciendo la premisa consuetudinaria de que la población civil debe gozar de protección general contra los efectos de las hostilidades, tal y como se refleja en el art. 48 del PA I. De esta opinión es, en particular, Nils Melzer[71], quien afirma que, a los efectos del «targeting», la respuesta correcta es, probablemente, la de que los datos deberían ser considerados como un objeto que no puede ser directamente atacado a menos que reúna los elementos propios de un objetivo militar, y que el borrado o modificación inevitable, aunque incidental, de datos civiles en el curso de una operación que persiguiera otra finalidad tendrían que ser evaluados conforme al principio de proporcio-

[71] Vid, *supra,* op. cit. en nota 44.

nalidad, de modo que, por ejemplo, la naturaleza potencialmente temporal del daño infligido pueda ser debidamente tenida en cuenta.

En cuanto a la aplicación a las ciberoperaciones de los criterios que, conforme al art. 52.2 del PA I, sirven para determinar la condición de objetivo militar de un objeto (naturaleza, ubicación, finalidad y uso), siguiendo al *Manual de Tallin* podemos resaltar brevemente los siguientes aspectos:

1.º *Naturaleza:* se refiere a aquellos objetos que son típicamente militares y están diseñados para contribuir a la acción militar. De especial importancia en el contexto cibernético son los sistemas C^4ISR *(command, control, communications, computer, intelligence, surveillance, reconnaisance),* que son esencialmente objetivos militares independientemente del hecho de que personas civiles (empleados gubernamentales o contratistas privados) puedan participar en su manejo.

2.º *Ubicación:* el hecho de que un objeto por razón de su situación contribuya efectivamente a la acción militar lo cualifica como objetivo militar. Así, por ejemplo, una ciberoperación contra el sistema SCADA de un depósito de agua podría utilizarse para inundar un área en la que opera militarmente el enemigo.

3.º *Finalidad:* un objeto adquiere la condición de objetivo militar tan pronto como se conoce con claridad que se utiliza o va ser utilizado con un propósito militar. El problema aquí radica a menudo en determinar la intención del enemigo.

4.º *Uso:* cuando un objeto o instalación civil se utiliza para fines militares, los mismos devienen en objetivos militares independientemente de que continúen también usándose para su propósito civil. Así, por ejemplo, podrían convertirse en objetivos militares y, por tanto, ser susceptibles de un ciberataque, redes ferroviarias civiles usadas por las fuerzas armadas o aeródromos civiles utilizados por aeronaves militares.

Con relación, precisamente, a los objetos de «doble uso», incluyendo ordenadores, redes de comunicaciones y ciberinfraestructuras, el *Manual de Tallin* recoge la regla de que son objetivos militares, con independencia de que a la hora de lanzar un ataque contra los mismos deban tenerse en cuenta tanto el principio de proporcionalidad que, conforme al art. 51.5 del PA I, prohibiría aquellos ciberataques que fuera de prever causarían incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista, como la exigencia de adoptar las debidas precauciones en el ataque para, de acuerdo con el art. 57.1 del PA

I, preservar de sus efectos a la población civil, a las personas civiles y a los bienes de carácter civil.

Las ciberoperaciones, se dice también en el manual, plantean retos especiales a este respecto. Piénsese en una red usada tanto para fines civiles como militares. Podría llegar a ser imposible saber sobre qué parte de esa red van a pasar las transmisiones militares. En tales casos, sería la red entera la que constituiría un objetivo militar.

En cuanto al uso de las redes sociales para fines militares, también aparece contemplado en el manual, en el que se citan los casos reales de la utilización de Facebook para la organización de operaciones de resistencia armada y de Twitter para la transmisión de información de valor militar. A este particular respecto, se señala que ha de tenerse en cuenta: 1) que siempre será necesario respetar el principio de proporcionalidad y el requerimiento de adoptar las debidas precauciones en el ataque; 2) que la legalidad de una ciberoperación contra una red social dependerá de si dicha operación tiene la consideración de ataque puesto que, en caso, contrario, ningún sentido tiene hablar aquí de objetivos militares; 3) que, por el hecho de que se usen para fines militares, ni Facebook ni Twitter, como tales, son susceptibles de ataque, siéndolo únicamente aquellos de sus componentes que se utilizaran con un propósito militar.

Otro supuesto problemático que se cita en el manual es, finalmente, el de aquellos sistemas para uso civil que generan imágenes o datos de localización, que serían también útiles para las fuerzas armadas durante un conflicto armado. Aquí también, en aplicación del principio de proporcionalidad y del requerimiento de adoptar las debidas precauciones, si fuera factible, dice el manual, la degradación, denegación de uso, perturbación o alteración de las señales en cuestión mediante una ciberoperación que no llegara al nivel de ciberataque, así habría que hacerlo en virtud de lo establecido en el art. 57.2 del PA I, que obliga a reducir en todo lo posible los daños a los bienes de carácter civil.

6.5. «Ciberguerreros»

En este punto, con el que concluiremos esta aproximación a las principales cuestiones que plantea la aplicación a las ciberoperaciones del DIH, seguiremos una vez más a Nils Melzer, para distinguir entre los siguientes grupos:

1.º. *Combatientes:* las ciberoperaciones son por lo general realizadas por personas altamente especializadas y, en la medida en que dichas per-

sonas sean miembros de las fuerzas armadas de un beligerante, su estatus no será distinto del de los combatientes tradicionales. Como tales, gozarán de la condición de prisioneros de guerra en caso de caer capturados por el enemigo y disfrutarán de la llamada «inmunidad del combatiente», lo que significa que no podrán ser enjuiciados por los actos de beligerancia que lícitamente hayan realizado conforme al DIH. Ha de tenerse en cuenta, sin embargo, como señala el *Manual de Tallin,* que en los conflictos armados no internacionales esta inmunidad no resulta de aplicación, por lo que serán las normas internas estatales las que determinarán la medida en que el responsable de un acto realizado en el marco de tal tipo de conflictos quedará exento de responsabilidad. Así, por ejemplo, si un miembro de las fuerzas armadas o de las fuerzas oponentes «hackea» los sistemas de comunicación del adversario, será la legislación interna del Estado la que determine la legalidad de tal acción.

2.º *Leva en masa:* es este un concepto con el que tradicionalmente se alude a los habitantes de un territorio no ocupado que se alzan espontáneamente en armas frente a un invasor extranjero, sin haber tenido tiempo para organizarse en unidades armadas regulares, los cuales, siempre que porten las armas abiertamente y respeten las leyes y usos de la guerra, gozarán tanto del estatus de prisioneros de guerra en caso de captura, como de la inmunidad del combatiente. Si bien Melzer señala que esta categoría, sin apenas relevancia en la guerra tradicional actual, podría, sin embargo, adquirirla en el contexto de la ciberguerra, en el *Manual de Tallin* se expresan ciertas dudas al respecto. Así, se señala, los medios y conocimientos necesarios para realizar efectivamente ciberoperaciones son relativamente limitados entre la población, siendo incierto que la leva en masa pueda estar integrada solamente por esa porción de miembros de la población que cuentan con esos medios y conocimientos.

3.º *Contratistas y empleados civiles:* el creciente fenómeno del empleo de contratistas privados y de empleados gubernamentales civiles para desarrollar ciertas funciones que tradicionalmente han sido propias de las fuerzas armadas, no ha podido menos que extenderse también al campo de las ciberoperaciones. De hecho, como hace notar William H. Boothby[72], existe una alta probabilidad de que este tipo de personal civil tome parte en ciberhostilidades. En el *Manual de Tallin* se plantea, por ejemplo, el caso de la contratación de una compañía privada por una parte en un conflicto para ejecutar operaciones militares específicas tales como ciberataques contra el enemigo. Para la mayoría de los expertos, esta compañía consti-

[72] Vid. *supra, op. cit.,* en n. 67.

tuiría un grupo armado organizado perteneciente a dicha parte, por lo que entrarían dentro de la segunda categoría de combatientes que, además de los miembros de las fuerzas armadas, se contempla en el DIH. Por el contrario, una minoría de expertos opinó que la relación contractual no sería suficiente base para ello.

4.º *Miembros de grupos armados organizados:* en los conflictos armados no internacionales, estos grupos constituyen las fuerzas armadas de una parte beligerante no estatal. Los individuos que realicen ciberoperaciones en nombre de esa parte beligerante no estatal perderán, entonces, su condición de civiles, para ser considerados miembros de un grupo armado organizado de esa parte, siempre y cuando conduzcan sus operaciones de una manera continua y que las mismas impliquen tomar parte directa en las hostilidades.

7. CONCLUSIONES

De una forma, lo reconocemos, un tanto apresurada, hemos dedicado el presente trabajo al fenómeno de la ciberguerra, presentándolo, inicialmente, en crudo, a partir del modo en que el mismo aparece reflejado en los medios de comunicación, sazonándolo, después, con las reflexiones de mayor calado que han tratado de acotar científicamente el concepto y, cocinándolo, finalmente, de manera algo más detenida, en el horno del Derecho Internacional.

La lectura de lo escrito creemos permite extraer una primera conclusión, ciertamente un tanto obvia, cual es la de que ese ámbito artificial al que hemos dado en denominar ciberespacio, que en verdad ha revolucionado las vidas de quienes nacimos antes de que los seres humanos comenzáramos a movernos cotidianamente en el mismo, puede ser también usado para hacer el mal. Es lo que, al parecer, acaba inevitablemente ocurriendo en aquellos ámbitos en los que, como secularmente ha sucedido en la alta mar (otro de los *global commons*), la actividad humana se ha regido por el principio de libertad. Y, del mismo modo en que el mal uso de ese espacio líquido de libertad para realizar todo tipo de actividades ilícitas condujo en su día al nacimiento y desarrollo de una creciente preocupación por la seguridad marítima, traducida en iniciativas diversas que han determinado que ese «eterno compromiso entre la libertad y la seguridad» a que se refiere Ángel Gómez de Ágreda[73], no haya tenido más remedio que ajustarse

[73] Gómez de Ágreda, Á., «El ciberespacio como escenario de conflictos. Identificación de amenazas», CESEDEN, n.º 126, 2012; véase n. 2.

en alguna medida para fortalecer al segundo de los factores, también en el ciberespacio hemos visto nacer y dar los primeros pasos a una, ya galopante, preocupación por la ciberseguridad.

Las posibilidades que el ciberespacio ofrece para hacer daño no solo a ciudadanos y empresas, sino también a los propios estados, atacando sus intereses más vitales, ha llevado a que, como no podía ser otra forma, esa ciberseguridad haya ido adoptando, junto a otras, una importante dimensión de ciberdefensa. Las fuerzas armadas que, como todos, son cada vez más ciberdependientes, no tienen más remedio que proteger y fortalecer sus redes, sistemas e infraestructuras para no ver mermada, o incluso anulada, su capacidad para actuar. Además, en cuanto depositarias de ese uso legítimo de la fuerza que monopoliza el Estado, deben estar también preparadas para, tanto en el ciberespacio como fuera de él, dar cumplida respuesta a los ataques que contra los más importantes intereses nacionales puedan provenir del ciberespacio.

El uso de la fuerza en el ciberespacio ha llevado de esta forma a la necesidad de determinar si tal uso de la fuerza debe estar en alguna medida limitado por el Derecho. Aunque, como hemos visto, hay quien responde negativamente a esta pregunta, la respuesta casi unánime es la afirmativa, pese a que luego existan discrepancias en cuanto a la senda a seguir en ese empeño. En nuestra opinión, sin perjuicio de que puedan explorarse vías como la de un tratado de control de las *ciberarmas* (una desmilitarización completa del ciberespacio nos parece a estas alturas una aspiración ilusoria), la opción más razonable es la de estimar plenamente aplicables en este ámbito las normas convencionales y consuetudinarias que conforman ese *ius ad bellum* y ese *ius in bello* que, tras un largo proceso histórico de decantación, constituyen parte integrante del acervo jurídico de la comunidad internacional.

Surge, entonces, una nueva necesidad, cual es la de interpretar adecuadamente esas normas, que fueron elaboradas en unas épocas en las que ni el uso de la ciberfuerza *(ius ad bellum)* ni las ciberhostilidades o ciberguerra *(ius in bello)* pudieron preverse ni, por tanto, regularse de manera expresa. El esfuerzo colectivo más importante realizado a tal fin hasta la fecha en el campo puramente doctrinal (por mucho que se encuentre institucionalmente avalado), el *Manual de Tallin* sobre el Derecho Internacional aplicable a la ciberguerra, ha servido para poner de manifiesto que esa no es una tarea sencilla. Las peculiaridades únicas del ciberespacio determinan que las discrepancias sean numerosas.

Hasta el momento, afortunadamente, no se han hecho realidad esas visiones apocalípticas que reflejan las expresiones de «Cyber-Pearl Harbor»

y, la todavía más dramática, de «Cybergeddon». Acontecimientos como los de Estonia en 2007 y Georgia en el 2008 y, en especial, ciberoperaciones como la llevada a cabo por medio del gusano informático STUXNET contra el programa nuclear de Irán, nos muestran, sin embargo, que los ciberataques son una realidad, tanto al margen como en el contexto de un conflicto armado. Partiendo del Derecho Internacional existente, la práctica estatal y, en su caso, la jurisprudencia de los tribunales internacionales deberán ir aclarándonos el panorama. Entretanto, y finalizamos citando de nuevo a Nils Melzer, el enorme potencial que para producir una tragedia humana poseen las ciberarmas debe llevar a que los responsables estatales se preocupen no solo de su deber jurídico de examinar si las nuevas armas y los nuevos métodos empleados en la ciberguerra serían compatibles con sus obligaciones conforme al DIH, sino también de su responsabilidad moral hacia las generaciones venideras.