# La ciberseguridad: aspectos jurídicos internacionales

## *Cyber security: international legal aspects*

JERÓNIMO DOMÍNGUEZ BASCOY
*Coronel Auditor del Cuerpo Jurídico Militar*



**RESUMEN.** El ciberespacio, ese relativamente nuevo entorno virtual en el que se desarrolla gran parte de nuestras vidas, no está en absoluto libre de amenazas, como los medios de comunicación nos muestran a diario. Los ideales ciberlibertarios, con su visión del ciberespacio como un lugar inmune a la acción estatal, quedaron pronto arrumbados, entre otras razones por la necesidad de hacer frente a esas amenazas, ya procedan de cibercriminales, de cibervándalos, de ciberterroristas o, incluso, de los propios Estados. La ciberseguridad, inicialmente una disciplina de carácter técnico, ha pasado a conformar, así, un elemento esencial en las estrategias de seguridad nacionales. Desde el punto de vista del Derecho internacional, el único avance producido para dotar de una regulación específica al ciberespacio es el que ha tenido lugar en el campo de la lucha contra la cibercriminalidad, mediante el Convenio de Budapest de 2001. Por lo demás, parece existir consenso acerca de que los principios y normas del Derecho internacional preexistentes son aplicables a la conducta de los Estados en el ciberespacio, particularmente, en lo que se refiere a la amenaza o al uso de la fuerza y a la conducción de ciberhostilidades en caso de conflicto armado. Las medidas de fomento de

la confianza constituyen, por su parte, un instrumento necesario para evitar una escalada de tensión en lo que se ha dado en llamar "ciberguerra fría".

**ABSTRACT.** The cyberspace, a relatively new virtual environment in which we live a great part of our lives, is by no means a threat-free zone, as the media show day by day. The cyber libertarian ideals, and its cyberspace vision as a place immune from state action, were soon cast aside, for some reasons including the need to deal with those threats, whether they come from cyber criminals, from cyber vandals, from cyber terrorists, or, even, from States. Cybersecurity, an initially technical discipline, has thus become an essential element in most of national security strategies. From the international law point of view, the only tailored rules for cyberspace are those contained in the Budapest Convention 2001, focused on combating cybercrime. Otherwise, some consensus can be seen on the applicability of pre-existing international law principles and rules to the conduct of states in cyberspace, particularly those related to the threat or use of force and the conduct of ciberhostilidades during an armed conflict. Confidence-building measures in cyberspace are, meanwhile, a necessary tool to avoid an escalation of tension in what has been called a "cold cyberwar".

**Palabras clave.** Ciberespacio, ciberseguridad, ciberoperaciones, soberanía territorial, diligencia debida, no intervención, contramedidas, *ius ad bellum*, ciberataque armado, legítima defensa, ciberespionaje, *ius in bello*, medidas de fomento de la confianza.

**Key words.** Cyberspace, cyber security, cyber operations, territorial sovereignty, due diligence, non-intervention, countermeasures, *ius ad bellum*, armed cyberattack, self-defense, cyber espionage, *ius in bello*, confidence-building measures.

## 1. INTRODUCCIÓN

### 1.1. EL CIBERESPACIO: CONCEPTO, ESTRUCTURA Y DEBATES ACERCA DE SU REGULACIÓN

Ciberguerra, ciberespionaje, ciberterrorismo, ciberdelito y otros cuantos términos más cuyo común denominador es ese prefijo "ciber", no son sino actividades que, de una u otra forma, afectan a lo que se ha dado en denominar "ciberseguridad". Es obvio que aquí la única novedad reside en lo que, para cada uno de esos términos, implica el citado prefijo. La guerra, el espionaje, el terrorismo, el delito y la seguridad son todos ellos conceptos bien conocidos en el mundo tangible, material, en el mundo "de carne y acero", tomando prestada la célebre expresión de John Perry Barlow[1].

1. Barlow, John Perry. *A Declaration of the Independence of Cyberspace* (1996). La declaración puede consultarse en: *https://projects.eff.org/~barlow/Declaration-Final.html.* Una traducción de la misma al español puede obtenerse en: *http://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf.*

A lo que el prefijo "ciber" remite es, entonces, a ese otro mundo virtual en el que o, mejor, a través del que también pueden desarrollarse hostilidades, realizarse actos de espionaje o acciones terroristas, así como cometerse una variada tipología de delitos: el ciberespacio.

Son variadas las definiciones que se han formulado del ciberespacio, término cuya paternidad se atribuye al autor del género ciberpunk William Gibson, quien en su novela "Neuromante"[2] describe aquél como una "alucinación consensual". De esta inicial conceptuación de Gibson se ha pasado, como señala Aguirre Romero[3], a un mundo virtual, por un lado, pero real por otro, si entendemos como real un mundo en el que es posible realizar acciones y tomar decisiones.

En contraste con los espacios terrestre, marítimo y aéreo, así como con el espacio exterior, el ciberespacio es una creación humana con componentes que pueden cambiar a través del tiempo. En la que constituye la estrategia nacional de ciberseguridad pionera, la Estrategia Nacional para la Seguridad del Ciberespacio (2003) de los Estados Unidos[4], se describe el ciberespacio como el "sistema nervioso" que controla las infraestructuras críticas del país. Al tiempo que pone de relieve el papel de la interconexión entre los sectores público y privado en este campo, la Estrategia señala que "el ciberespacio se compone de cientos de miles de ordenadores, servidores, routers, conmutadores y cables de fibra óptica interconectados, que permiten operar a nuestras infraestructuras críticas, por lo que el funcionamiento saludable del ciberespacio resulta esencial tanto para nuestra economía como para nuestra seguridad nacional".

En España, la primera definición oficial que se ha formulado del ciberespacio es la que se contiene en la Orden Ministerial 10/2013, de 19 de febrero, por la que se creó el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, en la que aquél es descrito como el "dominio global y dinámico compuesto por infraestructuras de tecnología de la información –incluyendo Internet–, redes de telecomunicaciones y sistemas de información". Unos meses después, en diciembre de 2013, esa misma definición fue replicada en la Estrategia de Ciberseguridad Nacional[5], la cual comienza por reconocer que el desarrollo de las Tecnologías de Información

2. Gibson, William. *Neuromante* (1984). Editada en español por Minotauro en su colección de Clásicos.
3. Aguirre Romero, Joaquín Mª. *Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI.* (2004). Espéculo. *Revista de estudios literarios.* Universidad Complutense de Madrid.
4. *The National Strategy to Secure Cyberspace.* Washington, DC. White House (2003).
5. Accesible en: *http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf.*

y Comunicación (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo. Circunstancia esta acerca de la que ya se había llamado la atención por parte de la doctrina. Así, García Mexía[6] señaló acertadamente cómo el impacto de la Red en nuestro hasta hace poco "sólo analógico" mundo ha sido tan grande, que las mismas circunstancias de tiempo y espacio han venido a quedar en mayor o menor medida afectadas. En cuanto al *tiempo,* señala dicho autor que algunos de los usos de la Red (piénsese en el envío de un correo electrónico) anulan sencillamente la noción de tiempo, al reducir su extensión a niveles prácticamente despreciables. Y, por lo que a la dimensión *espacial* respecta, pone de relieve García Mexía, citando a Dan Hunter[7], que, por mucho que considerar al ciberespacio como un lugar no sea más que una metáfora, lo cierto es que ésta ha hallado pleno eco en nuestro sistema cognitivo, que continuamente recurre a vocablos e ideas relacionados con el espacio físico para parangonarlos con los propios de Internet.

Seguramente, la mejor forma de entender el ciberespacio sea la que lo conceptualiza atendiendo a las diferentes capas interdependientes que lo conforman. Siguiendo a David Clark[8], podemos captar la esencia de aquél utilizando un modelo construido sobre cuatro capas. Son éstas:

1ª. La capa física.

Base fundacional del ciberespacio[9], está constituida por los dispositivos físicos a partir de los cuales aquél se encuentra construido. El ciberespacio es, de esta forma, un espacio conformado por dispositivos informáticos interconectados, por lo que sus elementos básicos son los PCs, servidores, supercomputadores, redes, sensores y transductores, así como Internet y otros tipos de redes y canales de comunicación. La capa física es, quizás, la más fácil de comprender ya que, al ser tangible, su propia fisicidad le dota de un sentido de la ubicación. Por otra parte, el hecho de que toda esta infraestructura física se encuentre situada en el espacio real determina que

6. García Mexía, Pablo. *Derecho Europeo de Internet* (2009). Editorial Netbiblo.
7. Hunter, Dan. *Cyberspace as a Place and the Tragedy of the Digital Anticommons* (2003). California Law Review, vol. 91, pp. 439 a 519.
8. Clak, David. *Characterizing cyberspace: past, present and future* (2010). MIT/CSAIL *Working Paper.*
9. Que la capa física constituye el presupuesto necesario para la propia existencia del ciberespacio fue, claramente, puesto de manifiesto en marzo de 2011, cuando una anciana georgiana dejó durante varias horas *offline* a Armenia, al cortar los cables de fibra óptica que unen Georgia con Armenia mientras hurgaba en busca de cobre. La noticia se puede ver, entre otros, en el siguiente enlace: *http://www.elmundo.es/elmundo/2011/04/06/internacional/1302119883.html.*

la misma pueda quedar sujeta a la jurisdicción nacional de cada uno de los Estados sobre cuyo territorio se localiza.

2ª. La capa lógica.

Como señalan KLIMBURG y MIRTL[10], esta capa se refiere generalmente al *código*, el cual incluye tanto al software como a los protocolos que dicho software lleva incorporados. Explicado a grandes rasgos, mientras los protocolos definen las reglas o convenciones precisas para obtener un objetivo determinado (por ejemplo, establecer una comunicación), el software es el programa informático que implementa dichos protocolos.

Según el citado CLARK, el diseño de Internet conduce a un ciberespacio construido a partir de componentes que proporcionan servicios, y estos servicios están diseñados de forma que puedan, a su vez, combinarse entre ellos para dar lugar a servicios de todavía mayor complejidad. Es, así, consustancial al ciberespacio la continua y rápida evolución de nuevas capacidades y servicios, basados en la creación y combinación de nuevos constructos lógicos. En definitiva, el ciberespacio puede describirse en este nivel lógico como una serie de plataformas sobre cada una de las cuales se desarrollan unas capacidades que, a su vez, devienen en plataformas para sucesivas innovaciones.

Ahora bien, esta abundancia de capacidades tiene también su lado oscuro, que no es otro, según alertan los citados KLIMBURG y MIRTL, que el *malware* o software malicioso, el cual incluye diferentes variedades de troyanos, virus y gusanos.

3ª. La capa semántica.

Denominada también capa de los contenidos o capa de la información, incluye todo aquello que es creado, capturado, almacenado y procesado dentro del ciberespacio: mensajes de correo electrónico, música, películas, libros, noticias, etc.

4ª. La capa social.

Es la que se encuentra conformada por todas las personas que se mueven en el ciberespacio y que dan forma a éste. La capa social incluye tanto a actores del sector público como del privado, pero tanto unos como otros comparten, como señalan KLIMBURG y MIRTL, una característica específica: mientras en la vida real las personas pueden ser en última instancia identificadas por su ADN único, la atribución de los actos es mucho más difícil en la vida ciberespacial donde, por un lado, una sola persona puede

10. KLIMBURG, Alexander y MIRTL, Philipp. *Cyberspace and Governance-A Primer* (2012). Austrian Institute for International Affairs *Working Paper* nº 65.

actuar con múltiples identidades y, por otro, una misma identidad virtual puede ser utilizada por múltiples usuarios.

Todas estas cuatro capas son importantes desde el punto de vista de la ciberseguridad por cuanto las ciberamenazas pueden dirigirse tanto hacia la capa física (destruyendo o dañando sus componentes), como hacia la capa lógica (infectándola con software malicioso), como hacia la capa semántica (comprometiendo la información) o hacia la capa social (corrompiendo a los usuarios).

Resta, finalmente, para cerrar este primer apartado introductorio, referirse someramente a los debates que, desde los mismos comienzos de la popularización de Internet, se han producido en torno a la regulación del ciberespacio. Los debates primigenios se centraron, claro está, en si este nuevo campo de actividad era susceptible de regulación o si, por el contrario, el ciberespacio constituía una suerte de *terra nullius* virtual. Esta última posición, basada en la creencia de que el ciberespacio debería ser ajeno a cualquier tipo de interferencia gubernamental, condujo a formular la idea de que aquél es, en efecto, un lugar inmune a la soberanía estatal. Sin duda, la formulación más radical de esta visión ciberlibertaria fue la realizada en 1996 por John Perry Barlow en su muy conocida Declaración de Independencia del Ciberespacio[11]. Con un lenguaje incuestionablemente seductor, Barlow arranca con fuerza en los dos párrafos iniciales de su Declaración:

> *"Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos.*
>
> *No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquélla con la que la libertad siempre habla. Declaro el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente".*

Desde el mundo del Derecho se defendió esta misma postura. Aunque con una retórica menos agresiva que la de Barlow, en el fondo el

11. Citada en la nota 1. La Declaración fue una reacción a la censura *online* introducida por la Communicatios Decency Act (1996), John P. Barlow, antiguo letrista del grupo de *acid rock* The Grateful Dead, fue uno de los cofundadores de la Electronic Frontier Foundation, organización dedicada a la defensa de los derechos civiles en la Red.

planteamiento era muy similar. Segura Serrano[12] señala, en este sentido, que la soberanía en el ciberespacio es la idea central en los escritos seminales de algunos autores como Johnson y Post[13]. Para éstos, las comunicaciones globales establecidas a través de ordenadores trascienden las fronteras territoriales, creando un nuevo ámbito de la actividad humana y socavando tanto la viabilidad como la misma legitimidad de la aplicación de las leyes basadas en fronteras geográficas. Surge, así, dicen, un nuevo límite, formado por las pantallas y las contraseñas que separan el mundo virtual del mundo real de los átomos. Este nuevo límite define un ciberespacio distintivo, que precisa y es capaz de crear unas instituciones jurídicas propias. Por mucho que las autoridades territoriales puedan encontrar este nuevo entorno profundamente amenazante, lo cierto es que deben aprender a ceder ante los esfuerzos de autorregulación de los participantes en el ciberespacio, quienes están más seriamente concernidos acerca de este nuevo comercio digital en ideas, información y servicios. De esta forma, ajenas a las jurisdicciones territoriales, surgirán nuevas reglas en una variedad de espacios en línea para gobernar una amplia gama de nuevos fenómenos que no tienen claro paralelismo en el mundo no virtual. Estas nuevas reglas tendrán la misma función que el Derecho mediante la definición de la personalidad jurídica y la propiedad y la solución de controversias, cristalizando en una conversación colectiva sobre valores fundamentales.

Esta visión ciberlibertaria ha sido combatida en sus vertientes descriptiva y normativa. Ante todo, se destaca que es harto cuestionable que el ciberespacio constituya, efectivamente, un espacio libre, una jurisdicción soberana ajena a todo control estatal. En segundo lugar, aun el supuesto de que se diera por buena esa afirmación, lo que el ciberespacio configurado a través de Internet era en sus inicios puede ser muy diferente de aquello en que es susceptible de evolucionar, tal y como Lawrence Lessig[14] ha puesto de manifiesto, señalando como, en contra de lo que imaginaban los pioneros de la Red y de su utopía de una Internet completamente libre e irregulable, el ciberespacio está a punto de convertirse en «el lugar más regulado que hayamos conocido jamás» como consecuencia no solo del potencial de control estatal, sino, en particular, de la propia la arquitectura (el código)

12. Segura Serrano, Antonio. *Internet Regulation and the Role of International Law* (2006). Max Planck Yearbook of United Nations Law, vol. 10, pp. 191-272.
13. Johnson, David R. y Post, David G. *Law and Borders –The Rise of Law in Cyberspace* (1996). Stanford Law Review, vol. 48, pp. 1367 y ss.
14. Lessig, Lawrence. *El código y otras leyes del ciberespacio* (1999). Editada en 2001 en español por Taurus. Una actualización de la obra original, *El código 2.0* (2006), editada en español por Traficantes de Sueños y publicada bajo licencia Creative Commons, puede descargarse gratuitamente desde*: http://www.traficantes.net/libros/el-codigo-20.*

de ese espacio. Por su parte, Jack L. GOLDSMITH[15] cuestionó la visión ciberlibertaria desde el ángulo normativo, afirmando no solo que la regulación del ciberespacio es viable y legítima, sino que las transacciones en aquél no son diferentes de las transacciones transnacionales que se producen en el "espacio real", existiendo razones fundadas para creer que las naciones pueden ejercer su autoridad territorial para lograr un control regulatorio significativo sobre las operaciones que tienen lugar en el ciberespacio.

Esos debates iniciales cedieron paulatinamente paso a una nueva ola doctrinal, habida cuenta de las múltiples formas en que gobiernos y corporaciones se fueron movilizando para regular y controlar las actividades *online*. No pudiendo ya defenderse seriamente la naturaleza inherentemente irregulable del ciberespacio, la doctrina viró hacia nuevas consideraciones centradas, fundamentalmente, en los modos en que cabe regular el comportamiento *online*. Como nos aclara Paul Schiff BERMAN[16], muchas personas piensan que tal regulación solo puede realizarse mediante instrumentos coercitivos, no reparando en el poder regulatorio del entorno y de la propia arquitectura del espacio en que actuamos. Pone este autor como ejemplo el hecho de que si, pongamos por caso, se deseara vetar el acceso de automóviles a un parque público, podría promulgarse una ordenanza prohibiendo tal conducta y organizando un sistema de vigilancia policial a fin de velar por el cumplimiento de la prohibición. Pero cabría, alternativamente, recurrir al sencillo expediente de colocar vallas que impidieran físicamente ese acceso. En ambos casos, tanto la ordenanza como las vallas operarían como herramientas regulatorias. Pues bien, sigue diciendo el citado autor, en el caso del ciberespacio es, precisamente, el segundo tipo de regulación el que habrá de ser, con probabilidad, prevalente, por cuanto la arquitectura del ciberespacio está, como hemos visto, determinada por el código del software, el cual es infinitamente maleable. Así, a través de sistemas de filtrado, el ciberespacio puede ser zonificado, creándose áreas en las que únicamente podrán entrar quienes poseen ciertas credenciales como una tarjeta de crédito o un número de identificación como adulto.

Una tercera ola de pensamiento en torno a la regulación del ciberespacio ha surgido en los últimos años, partiendo de las aportaciones de las dos precedentes. Piensan estos autores, de entre los que cabe destacar a Jonathan ZITTRAIN[17], que el ciberespacio posee, en efecto, elementos distintivos que

15. GOLDSMITH, Jack L., *Against Cyberanarchy* (1998). University of Chicago Law Review, nº 65 (otoño 1998), pp. 1199 y ss.

16. BERMAN, Paul Schiff. *Law and Society Approaches to Cyberspace* (2007). University of Connecticut School of Law Articles and Working Papers. Paper 72.

17. ZITTRAIN, Jonathan. *The Generative Internet* (2006). Harvard Law Review, vol. 119, p. 1974, May 2006; Oxford *Legal Studies Research Paper* nº 28/2006; Berkman Center Research Publication nº 2006/1.

abren la puerta a nuevas esferas de conexión y generan nuevas oportunidades tanto para la creación como para modificar la economía y la cultura política. Simultáneamente, están seriamente concernidos por las cuestiones relacionadas con la arquitectura técnica. Se orientan, de este modo, hacia la cuestión de cómo mantener el ciberespacio como un lugar en el que los usuarios puedan conservar la capacidad de desarrollar continuas adaptaciones e innovaciones frente a las tendencias a hacer de aquél algo que no vaya más allá de una serie de aparatos interconectados con una función específica bien delimitada, en lugar de ese espacio generativo que la maleabilidad esencial de su arquitectura permite libremente desarrollar.

## 1.2. LA CIBERSEGURIDAD: SU DIMENSIÓN ESTRATÉGICA

Según se constata en nuestra Estrategia de Ciberseguridad Nacional[18], ésta, la ciberseguridad, es una necesidad de nuestra sociedad y de nuestro modelo económico; por eso, dada la influencia de los Sistemas de Información y Telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad de nuestro país depende en buena medida de la seguridad y fiabilidad del ciberespacio, cualidades estas que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas.

Kenneth Geers[19] describe la evolución experimentada por la ciberseguridad, que de una disciplina puramente técnica ha pasado rápidamente a convertirse en un concepto estratégico. La globalización e Internet, señala, han proporcionado a los individuos, a las organizaciones y los Estados un poder increíble basado en el constante desarrollo de la tecnología de redes. Para todo el mundo –estudiantes, militares, espías, propagandistas, hackers o terroristas– la recolección de información o de fondos, las comunicaciones y las relaciones públicas se han digitalizado en forma verdaderamente revolucionaria. Pero esta digitalización, nos recuerda Marco Roscini[20] citando a un antiguo Subsecretario de Defensa de los Estados Unidos, es una espada de doble filo, por cuanto en este siglo XXI en el que nos encontramos "los bits y los bytes pueden llegar a ser tan amenazadores como las balas y las bombas".

18. Citada en la nota 5, constituye, no por casualidad, junto con la Estrategia de Seguridad Marítima Nacional, aprobada también en diciembre de 2013, la avanzadilla de las estrategias de segundo nivel, que desarrollan la Estrategia de Seguridad Nacional de mayo de 2013.
19. Geers, Kenneth. *Strategic Cyber Security* (2011). Publicación del NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).
20. Roscini, Marco. *Cyber Operations and the Use of Force in International Law* (2014). Oxford University Press.

El propio Roscini anuncia que la ciberseguridad está llamada a adquirir creciente importancia en los años venideros. La amenaza no procede ya, tan solo, del clásico hacker adolescente, sino también de individuos altamente ideologizados (hacktivistas), de Estados, de criminales y de organizaciones terroristas. Las tecnologías y destrezas cibernéticas son relativamente baratas y fáciles de obtener, permitiendo que Estados débiles e, incluso, actores no estatales puedan causar un daño considerable a Estados con un poderío militar considerablemente mayor.

En la ya citada Orden Ministerial 10/2013, de 19 de febrero, por la que se creó el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, la ciberseguridad es definida como el "conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan". Definición que debe, necesariamente, ponerse en relación con la que, inmediatamente antes, se formula de "ciberataque" como "acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan".

Siguiendo al citado Geers, explicaremos someramente a continuación esas tres formas básicas de ciberataque que los responsables del planeamiento de la seguridad nacional deben tomar en consideración.

Un primer tipo de ataque es el que se dirige contra la *confidencialidad* de los datos. Comprende cualquier adquisición no autorizada de información, incluso por vía de "análisis del tráfico", con el que el atacante deduce el contenido de la comunicación simplemente observando los patrones de comunicación. Puesto que, hoy por hoy, el grado de conectividad global en red es mucho más elevado que el grado de seguridad de la red, sea global o local, no resulta muy difícil la obtención no autorizada de enormes cantidades de información sensible. Un ejemplo célebre es el de *GhostNet* ("Red Fantasma"), nombre dado en 2009 a una gran operación de espionaje electrónico, cuyo origen mayoritario se centraba en la República Popular China. La red consiguió infiltrarse en unos 1.300 ordenadores en 103 países comprometiendo sistemas de embajadas y otras oficinas gubernamentales, así como también centros del exilio del tibetano en la India y en las ciudades de Bruselas, Londres y Nueva York[21].

Un segundo tipo de ataque es el que afecta a la *integridad* de la información, lo que incluye el sabotaje de los datos con propósitos criminales,

21. La noticia sobre esta red, divulgada por el *New York Times,* puede consultarse en: *http://tecnologia.elpais.com/tecnologia/2009/03/29/actualidad/1238320861_850215.html*.

políticos o militares. Se conocen casos de cibercriminales que han encriptado los datos de los discos duros de sus víctimas, exigiendo el pago de una suma de dinero a cambio de facilitarles la clave de desencriptación.

Una tercera modalidad es la de los ataques que se dirigen contra la *disponibilidad* de los sistemas o de la información contenida en los mismos. El objetivo es en este caso impedir que los usuarios autorizados tengan acceso a los sistemas o a los datos. Son lo que comúnmente se conocen como ataques de denegación de servicio, que comprenden un amplio espectro de software malicioso, tráfico de red o ataques físicos contra ordenadores, bases de datos y las redes que los conectan.

Por otra parte, el concepto emergente de "ciberseguridad nacional" se enfoca fundamentalmente, como señalan Melissa E. Hathaway y Alexander Klimburg[22], hacia la gestión doméstica de los riesgos procedentes del ciberespacio que las naciones han de encarar, más que hacia la expansión de su posición estratégica explotando de una manera proactiva esos riesgos para avanzar su poder global. Estos autores, basándose en el previo trabajo de Klimburg y Mirtl[23], recuerdan que al tratar sobre la ciberseguridad nacional es importante retener que ésta no constituye un área única, sino que debe dividirse en cinco perspectivas diferentes, cada una de los cuales puede ser afrontada por diferentes departamentos gubernamentales. Son dichas perspectivas:

1º. Las ciberactividades militares.

Nuestra citada Orden Ministerial 10/2013 define 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".

Como cometidos del Mando Conjunto de Ciberdefensa que por dicha Orden se crea se citan, entre otros, los de garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios; garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados; garantizar

22. Hathaway, Melissa E. y Klimburg, Alexander. *Preliminary Considerations: on National Cyber Security.* Capítulo I de la obra colectiva *National Cyber Security Framework Manual* (2012), editada por A. Klimburg y publicada por el NATO CCD COE.
23. *Vid*. nota 10.

el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques, y ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

No es, obviamente, solo en España donde se están desarrollando cibercapacidades militares, tanto defensivas como ofensivas. Desde hace unos años se habla de la existencia de una "carrera de armas virtual" en el ciberespacio. Según KLIMBURG y MIRTL esas capacidades pueden verse, simplemente, como un instrumento bélico más, similar a la capacidad derivada del poder aéreo, susceptible de ser utilizada solo en el marco de concretas misiones tácticas como, por ejemplo, para inutilizar un sistema de defensa aéreo previamente a lanzar un ataque convencional. Pero, alternativamente, señalan, el énfasis puede situarse en el superior nivel estratégico, de forma que esas capacidades se empleen para atacar a lo más esencial de una nación, socavando su economía y sus funciones más básicas. Cabría, así, pensar en una suerte de ciberguerra sin restricciones en la que se busque producir el máximo daño a las infraestructuras críticas del adversario, destruyendo el mismo tejido social de la nación. Los ejemplos frecuentemente citados son los referidos a ataques contra el sistema de control de tráfico aéreo, los sistemas de producción y distribución de energía, los servicios de emergencia y el sistema financiero.

2º. La lucha contra la cibercriminalidad.

El ciberdelito, considerado como una de las empresas criminales más rentables, comprende una variada panoplia de actividades criminales, algunas de las cuales no son sino conductas delictivas tradicionales que aprovechan este nuevo medio que es el ciberespacio para desarrollarse, mientras que otras constituyen nuevas formas de delincuencia asociadas al nacimiento de este nuevo espacio de interacción social.

Es en este campo donde, precisamente, nos encontramos con la, hasta ahora, única norma de Derecho Internacional específicamente relacionada con el ciberespacio. Se trata, claro está, del Convenio sobre la ciberdelincuencia (Budapest, 2001)[24], elaborado en el marco del Consejo de Europa. El Convenio no contiene una definición de lo que haya de entenderse por "ciberdelito", sino que opta por referirse, dentro de la parte correspondiente al Derecho penal sustantivo, a las diferentes conductas criminales que los Estados parte en el mismo deberán incorporar a su legislación interna. En este sentido, se distinguen los delitos contra la confidencialidad, la integridad

24. La versión en español puede consultarse aquí: *http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF*.

y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad de los sistemas y abuso de dispositivos), los delitos informáticos (falsificación informática y fraude informático), los delitos relacionados con el contenido (pornografía infantil) y, finalmente, los delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines.

Además de las disposiciones penales sustantivas, el Convenio de Budapest contiene normas procesales y jurisdiccionales, completándose con un detallado sistema de cooperación internacional en la lucha contra este tipo de delincuencia.

Los citados KLIMBURG y MIRTL advierten que, aunque las víctimas de los ciberdelitos sean generalmente los ciudadanos individuales o las corporaciones, desde el punto de vista de la seguridad nacional no puede perderse de vista la capacidad de apoyo logístico que el cibercrimen es capaz de ofrecer a cualquiera que esté interesado en la conducción de ciberataques. Así, el alojamiento de servicios, la venta de identidades falsas o de números de tarjetas de crédito robados, los servicios de blanqueo de dinero e, incluso, el suministro de completos *kits* de ataque[25]. Es en este punto donde, según dicen dichos autores, se produce la intersección del cibercrimen no solo con las ciberactividades militares, sino también con el ciberterrorismo. Este último es, dicen, un término altamente problemático, en cuanto pudiera ser indebidamente utilizado para criminalizar no solo esas conductas cibercriminales de menor gravedad conocidas como *hacktivismo*, sino incluso cualquier tipo de crítica política *online*. Solo deben, por tanto, considerarse ciberterrorismo aquellos actos ejecutados con medios cibernéticos en los que la destrucción ocasionada alcanza el nivel de un ataque terrorista convencional.

3º. Las actividades de inteligencia y contrainteligencia.

Si en febrero de 2013 nos quedamos atónitos ante las revelaciones contenidas en el Informe Mandiant[26] sobre las actividades de ciberespionaje de la unidad secreta 61398 del Ejército chino, no menor fue la sorpresa que causó la noticia, aparecida en mayo de 2014, de que la justicia de los Estados Unidos había imputado a cinco militares chinos por espionaje industrial a varias empresas del sector energético[27].

25. Véase, por ejemplo, la información que a este respecto proporcionó Symantec sobre que *"Los Kits de Herramientas para Realizar Ataques Cibernéticos Dominan el Entorno de Amenazas en Internet"*: *http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20110118_01*.
26. Véase al respecto la noticia tal como, entre otros medios, se recogió en *El País*: *http://internacional.elpais.com/internacional/2013/02/19/actualidad/1361276929_483540.html*.
27. Véase la noticia en: *http://internacional.elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html*.

El general Keith Alexander, entonces presidente de la Agencia de Seguridad Nacional de los Estados Unidos y comandante del cibercomando norteamericano, definió en 2013 el creciente problema del ciberespionaje industrial como "la mayor transferencia de riquezas de la historia", calculándose que las empresas estadounidenses sufrieron pérdidas estimadas en más de 300.000 millones de dólares en concepto de robos de secretos en el 2012.

Ello, por sí solo, pone de manifiesto la importancia del problema desde el punto de vista de la seguridad nacional. Problema que se agrava cuando la víctima del ciberespionaje es el propio Estado, lo que, desde el punto de vista de la política exterior, hace preciso desarrollar específicos mecanismos de respuesta capaces de hacer frente a la inherente ambigüedad que la autoría presenta en el ciberespacio. Al mismo tiempo, señalan Klimburg y Mirtl, las actividades de contrainteligencia (por ejemplo, las dirigidas a la detección de las ciberintrusiones más sofisticadas) dependerán muy a menudo de la recolección ofensiva de inteligencia, aunque también del intercambio de información entre socios internacionales.

En España, el CCN-CERT[28] es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN). Este servicio se creó a finales del año 2006 como el CERT (*Computer Emergency Response Team*) gubernamental/nacional, y sus funciones quedan recogidas en la Ley 11/2002, reguladora del Centro Nacional de Inteligencia, el Real Decreto 421/2004, que regula el CCN y en el Real Decreto 3/2010, regulador del Esquema Nacional de Seguridad. De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos. La misión del CCN-CERT es, por tanto, contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a las Administraciones Públicas y a las empresas estratégicas, y afrontar de forma activa las nuevas ciberamenazas.

4º. La protección de infraestructuras críticas y la gestión de crisis en el nivel nacional.

Como se dice en la página web de nuestro Centro Nacional para la protección de las infraestructuras críticas[29], la gran dependencia que la sociedad tiene del sistema de infraestructuras que aseguran el mantenimiento de los servicios esenciales, hace que su protección sea una prioridad para las diferentes naciones, situación en la que España no es una excepción.

28. Accesible en: *https://www.ccn-cert.cni.es/.*
29. Accesible en*: http://www.cnpic.es/Presentacion/index.html*.

La promulgación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (conocida como Ley PIC) responde, precisamente, a esas necesidades largamente demandadas por buena parte de los sectores público y privado de nuestro país. Más allá del cumplimiento de la normativa comunitaria, el fin primordial de la Ley, y la del reglamento que la desarrolla (Real Decreto 704/2011, de 20 de mayo), es el establecimiento a nivel nacional de una serie de medidas en materia de protección de infraestructuras críticas que proporcionen un soporte adecuado sobre el que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de dichas infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad global.

La citada normativa PIC destaca la necesidad de garantizar la adecuada prestación de los servicios esenciales a través de mecanismos que posibiliten una seguridad integral de las infraestructuras críticas sobre las que descansa la provisión de aquéllos. Con el objetivo concreto de reforzar los aspectos relativos a la ciberseguridad de dichas infraestructuras, se ha puesto en marcha un servicio de gestión de incidentes, el Centro de Respuesta a Incidentes de Seguridad en Infraestructuras Críticas, encargado de gestionar dichos incidentes desde su notificación inicial, hasta su cierre, pasando por el ciclo de vida definido en el correspondiente procedimiento.

Según KLIMBURG y MIRTL, si bien el foco original de los programas de protección de infraestructuras críticas era a menudo el terrorismo, actualmente la mayor parte de la actividad PIC está directamente conectada con el ciberespacio (normalmente, cibercrimen y ciberespionaje). Señalan, además, que, en este contexto, los sistemas nacionales de gestión de crisis deben necesariamente contar con un cibercomponente, lo que incluye establecer estructuras institucionales que refuercen la cooperación entre actores estatales y no estatales tanto nacional como internacionalmente, una red estable de comunicación para las situaciones de crisis y un marco jurídico que permita el intercambio de información relevante.

El capítulo 5 de nuestra Estrategia de Ciberseguridad Nacional se dedica, precisamente, a enmarcar la ciberseguridad dentro del sistema de seguridad nacional. La estructura orgánica creada a estos efectos está constituida por los siguientes componentes bajo la dirección del Presidente del Gobierno:

– El Consejo de Seguridad Nacional, configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, que asiste al Presidente del Gobierno en la dirección de la política de seguridad nacional.

– El Comité Especializado de Ciberseguridad, que dará apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en

particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Además, reforzará las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

– El Comité Especializado de Situación, que será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad que, atendiendo a la acentuada transversalidad o dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos habituales previstos, con el fin de garantizar una respuesta inmediata y eficaz a través de un solo órgano de dirección político-estratégica de la crisis.

5º. La ciberdiplomacia y el gobierno de Internet.

KLIMBURG y MIRTL comienzan en este punto citando la frase de Evan H. POTTER[30] acerca de que la ciberdiplomacia versa acerca de "como la diplomacia se está adaptando al nuevo orden global de la información".

Numerosas conferencias y reuniones sobre el ciberespacio, patrocinados por gobiernos y organizaciones internacionales, se están llevando a cabo con el fin de discutir las respuestas políticas, técnicas, educativas y jurídicas a los desafíos cibernéticos. Concretamente, en lo que más directamente afecta a la ciberseguridad, la cuestión relativa a "los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional" ha estado en el programa de las Naciones Unidas desde 1998, cuando la Federación Rusa presentó una resolución en la Primera Comisión de la Asamblea General de las Naciones Unidas. Desde entonces ha habido informes anuales del Secretario General a la Asamblea General en la que los Estados miembros de las Naciones Unidas han expresado sus puntos de vista sobre este asunto, haciendo hincapié en la necesidad de llevar a cabo una acción colectiva.

KLIMBURG y MIRTL señalan que, mientras la ciberdiplomacia es algo similar a otros esfuerzos diplomáticos sobre temas tales como el control de armamentos o la contra-proliferación, el gobierno de internet es una actividad que implica tanto a los gobiernos como a la sociedad civil. Se refiere generalmente al proceso por el cual diversos Estados y actores no estatales interactúan en la gestión de lo que constituye esa capa lógica del

30. POTTER, Evan H., *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (2002). McGill-Queen's University Press.

ciberespacio a que anteriormente nos referíamos. La emergencia del debate actual en torno al gobierno de Internet se sitúa, según García Costa[31], en el contexto de la configuración de Internet como bien público global y de la aparición de la ICANN (*Internet Corporation for Asigned Names and Numbers*) como organismo encargado de gestionar algunas cuestiones clave de Internet. Como señala este autor, la mera existencia de la ICANN, al fin y al cabo un órgano vinculado a las autoridades norteamericanas, ha sido el catalizador que ha convertido la cuestión del gobierno de Internet en uno de los fundamentales de las agendas de los Gobiernos de los diferentes Estados. Si Internet es un bien público global, todas las cuestiones fundamentales de política pública de la misma deberían ser consensuadas por todos los actores de la red, especialmente las relacionadas con la creación de cualquier tipo de estructura de poder como la ICANN.

Habida cuenta de todo lo anterior, no resulta en modo alguno extraño que la ciberseguridad haya ido encontrando hueco en las estrategias de seguridad y defensa nacionales de numerosos Estados, así como que hayan proliferado documentos estratégicos específicamente dedicados a aquélla[32]. Y tampoco puede extrañar que tanto la Unión Europea como la OTAN cuenten con documentos políticos y estratégicos al respecto.

En el caso de la primera, la aprobación de la Estrategia de Ciberseguridad de la Unión Europea, "Un Ciberespacio Abierto, Protegido y Seguro"[33], tuvo lugar en febrero de 2013 mediante una comunicación conjunta de la Comisión Europea y de la Alta Representante de la UE para Asuntos Exteriores y Política de Seguridad. En la misma se proclaman los principios que han de presidir la política de ciberseguridad tanto en la UE como a escala internacional: el reconocimiento de que los valores esenciales de UE lo son tanto en el mundo físico como en el digital; la protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad; el acceso para todos; una gobernanza multilateral democrática y eficaz, y la garantía de la seguridad como responsabilidad compartida. La visión de la UE que se presenta en la estrategia se articula en torno a cinco prioridades estratégicas: lograr la ciber-resiliencia, reducir drásticamente la ciberdelincuencia, desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD), desarrollar recursos industriales y tecnológicos de ciberseguridad y establecer una

31. García Costa, Francisco M., *El gobierno de Internet como reto del Derecho Constitucional* (2006). *Anales de Derecho de la Universidad de Murcia*, nº 24, pp. 267 a 289.

32. En la página web del Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN, con sede en Tallin (Estonia), pueden consultarse hasta las de 53 Estados: *https://ccdcoe.org/strategies-policies.html*.

33. Accesible en: *http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20130001.do.*

política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE.

Por su parte, la OTAN aprobó en septiembre de 2014, durante la cumbre celebrada en Cardiff (Gales), su nueva política mejorada de ciberdefensa[34]. La OTAN reconoce que el Derecho Internacional, incluyendo el Derecho Internacional Humanitario y la Carta de las Naciones Unidas, se aplica al ciberespacio, y que la ciberdefensa forma parte integrante de la tarea principal de defensa colectiva de la OTAN. Por lo tanto, el artículo 5 del Tratado del Atlántico Norte, la cláusula relativa a la legítima defensa colectiva, podría llegar a invocarse en el caso de un ciberataque con efectos comparables a los de un ataque armado convencional.

### 1.3. IDEAS BÁSICAS ACERCA DE LAS CIBEROPERACIONES

Siguiendo la explicación que nos proporciona Markus Maybaum[35], la actividad de los actores estatales en el ciberespacio no se centra exclusivamente en la seguridad de las TIC (tecnologías de la información y las comunicaciones) y en escenarios de ciberdefensa. Diferentes órganos estatales han encontrado en el ciberespacio un nuevo dominio de participación. De esta forma, la policía, los servicios de inteligencia y las Fuerzas Armadas operan habitualmente en el ciberespacio para cumplir con sus obligaciones: la investigación de sistemas sospechosos, las actividades de inteligencia o, incluso, el desarrollo de operaciones militares en tiempo de paz en el ciberespacio son ya una realidad. Estas actividades, englobadas genéricamente bajo el término de "ciberoperaciones", tienen algo en común: la irrupción en los sistemas TIC extranjeros para extraer o modificar datos, para cambiar la configuración del sistema e, incluso, para provocar su colapso. Para explicar de forma muy elemental estas actividades usaremos el modelo abstracto de ciberoperaciones que nos explica el citado M. Maybaum. Se trata, concretamente, del modelo de ciberoperaciones utilizado por el Departamento de Defensa de los EEUU, al que se conoce como *Cyber-Kill Chain* (CKC).

La intrusión en sistemas ajenos es lo que comúnmente se conoce como un ciberataque. La OTAN los define como "medidas adoptadas a través del uso de redes informáticas con el fin de interrumpir, negar,

34. Puede consultarse al respecto el Documento Informativo del Instituto Español de Estudios Estratégicos que firma David Ramírez Morán: *http://www.ieee.es/Galerias/fichero/docs_informativos/2014/DIEEEI13-2014_Ciberseguridad_CumbreGales_DRM.pdf.*

35. Maybaum, Markus. *Technical Methods, Techniques, Tools and Effects of Cyber Operations* (2013). Capítulo de la obra colectiva, editada por Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, publicada por el NATO CCD COE.

degradar o destruir tanto la información albergada en ordenadores y redes informáticas como los propios ordenadores y redes"[36].

Los ciberataques pueden ser analizados conforme a una serie secuenciada de pasos, comenzando con la etapa de preparación y terminando con la explotación, el mando y control o el ataque persistente, dependiendo de los objetivos de la misión. El citado modelo CKC distingue las siguientes fases en este tipo de operaciones: reconocimiento, desarrollo del vector de ataque, lanzamiento, explotación, instalación, mando y control y, finalmente, acción.

1º. Reconocimiento. Como cualquier otra operación, las ciberoperaciones deben planificarse sobre la base de una información adecuada y fiable. En el proceso de toma de decisiones debe, por tanto, recogerse información cuya integridad, autenticidad y exactitud esté garantizada a fin de poder obtener una sólida visión de la situación, a partir de la cual puedan evaluarse los diferentes cursos de acción. El proceso de recolección de esta información es lo que se conoce como *footprinting* (huella). La recopilación de la información disponible en fuentes abiertas o prestada por algún tipo de servicio es lo que se denomina "huella pasiva". La "huella activa" se referiría, por el contrario, a la actuación propia de obtención de la información que falta, y sería análoga a la actividad de "reconocimiento del campo de batalla". Como resultado de estas actividades de reconocimiento se obtendrá un cuadro detallado de la situación del sistema objetivo, que se actualizará continuamente en las subsiguientes etapas de la ciberoperación. Además, una vez que un intruso obtiene acceso al sistema objetivo, el panorama se enriquece con la información que se encuentra en el mismo o en otros sistemas intermedios utilizados para llegar hasta aquél.

2º. Desarrollo del vector de ataque. Una vez identificado el objetivo, conformada una visión de la situación y obtenida una huella digital de la red, la parte más difícil en la preparación de la misión es encontrar los medios adecuados para producir el efecto deseado en el objetivo. Se usa una gran variedad de términos para calificar a esos medios: "herramientas de hackeo", "*exploits*", "software malicioso" o, incluso, "ciberarmas". Nos hallamos, por tanto, en esa fase del proceso en la que se trata de identificar las herramientas cibernéticas adecuadas para lanzar un ciberataque contra un sistema. A tal fin se utilizan vulnerabilidades identificadas, configuraciones incorrectas o errores de los propios usuarios.

3º. Lanzamiento. En esta fase se produce la transferencia de la herramienta, *exploit* o como queramos llamarlo hacia el sistema de destino. En

36. NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-6), 2012.

principio, las opciones de los agentes estatales son en este punto limitadas, ya que deben garantizar que sus manipulaciones sólo afectan al sistema objetivo y no producen efectos secundarios, mientras que, por regla general, los hackers no estarán demasiado preocupados a ese respecto, siendo incluso normal que utilicen sistemas de terceros a modo de *proxies* para lanzar sus ciberataques. El lanzamiento hacia el sistema objetivo de lo que metafóricamente se denomina "carga explosiva" *(payload)* se puede automatizar. La forma más habitual de dispersión de cargas son los virus informáticos, que pueden ser diseñados para atacar sólo un sistema específico o para infectar cualquier sistema en el que sean descargados. El lanzamiento por *exploits* de servicios, especialmente por los llamados "gusanos", es también frecuente. La forma más sofisticada para la difusión de las cargas es el uso de los llamados *botnets*[37].

4º. Explotación. Uno de los requisitos más importantes para la explotación del sistema objetivo es la capacidad física para alterar el control de flujo de programa en el mismo. Una explotación exitosa proporciona un acceso privilegiado al sistema objetivo sin la necesidad de contar con credenciales de usuario. Los *exploits* se combinan principalmente con cargas que crean un canal de comunicación entre el intruso y el sistema objetivo. Las modificaciones producidas en el sistema por el *exploit* no son persistentes en esta etapa, ya que la carga queda únicamente almacenada en la memoria RAM. Para crear una "puerta trasera" permanente al sistema objetivo o para preparar y llevar a cabo las acciones previstas se requerirá la instalación de cargadores, herramientas de acceso u otro software malicioso. *Exploits* muy sofisticados pueden, incluso, borrar sus huellas tras el emplazamiento de la carga.

5º. Instalación. Una vez explotado con éxito el sistema objetivo o conseguido acceso al mismo debido a errores de configuración o a errores del usuario, las acciones maliciosas pueden exigir la instalación de software adicional, a menos que la misión pueda ejecutarse a través de la funcionalidad proporcionada por el propio sistema operativo del sistema objetivo o del software ya instalado. En la mayoría de casos, el software que se instala en el sistema objetivo es una "herramienta de acceso remoto" (RAT, por *Remote Access Tool*), permanentemente disponible en el proceso de

37. De acuerdo con D. Fischer, *What is a Botnet? (Botnet Definition)*, Kasperspy Lab (2013), un *botnet* es el nombre genérico que se da a una serie de ordenadores que se hallan controlados por un atacante remoto. Los *botnets* son generalmente creados por un atacante concreto o por un pequeño grupo de atacantes utilizando una pieza de *malware* para infectar un gran número de máquinas. Los PC individuales que forman parte de una red son conocidos como *"bots"* o *"zombis"*. Ejemplos de *botnets* que han surgido en los últimos años incluyen Conficker, Zeus, Waledac, Mariposa y Kelihos.

arranque del sistema y con la que se abre una "puerta trasera" que permite al intruso adquirir el control de aquél. Ocultar una RAT es el reto más importante ya que, en el caso de ser detectada, los administradores del sistema objetivo sabrán que éste ha sido hackeado y, lógicamente, adoptarán medidas tendentes a la eliminación de aquélla. Para fortalecer la capacidad de recuperación de una RAT se utilizan los denominados *rootkits*, los cuales se caracterizan por su capacidad para ocultar o eliminar cualquier rastro de la colocación, de las actividades y de la propia existencia de la RAT. Si un *rootkit* se ha instalado correctamente y no ha sido detectado y eliminado, el sistema objetivo pasará a ser controlado por el intruso, pudiendo llevar a cabo acciones maliciosas de todo tipo.

6º. Mando y control. Generalmente, el mando y control sobre el sistema objetivo se implementan a través de la comunicación en red. Dado que los sistemas protegidos tienden a controlar el tráfico de red y a analizarlo en busca de actividades sospechosas, el mando y control se suele esconder en canales secretos, donde la comunicación del intruso queda inserta en otra comunicación de red que no resulta sospechosa a los "cortafuegos" o a otros productos de seguridad instalados en el sistema objetivo. Además de la comunicación de red, también puede establecerse un sistema de mando y control *offline* en la propia herramienta utilizada para la intrusión. En este caso, una vez lanzada e instalada, dicha herramienta lleva consigo toda la información precisa para actuar en el sistema objetivo. Esta técnica se utiliza, sobre todo, cuando se lanzan las llamadas "bombas lógicas" contra un objetivo, las cuales no requieren de ningún canal de enlace con el intruso una vez han sido instaladas.

7º. Acción. Una vez que el intruso está en condiciones de dar órdenes sobre el sistema objetivo, las posibles acciones que cabe llevar a cabo son muy diversas: renombrar archivos, cambiar las versiones y fechas de los archivos, alterar cuadros y tablas en los documentos archivados, borrar archivos, modificar privilegios de usuario, cambiar contraseñas, desinstalar software, etc. Se han visto ya, incluso, casos de intrusión exitosa en los dispositivos de control industrial de ciertas infraestructuras que, como sucedió con el célebre gusano *Stuxnet*[38], pueden llegar al punto de causar daño físico a infraestructuras críticas. Éstas están, obviamente, bien protegidas, de modo que el desarrollo de herramientas diseñadas para su ataque requiere una gran cantidad de recursos en términos de expertos, presupuesto y pruebas, lo que limita significativamente el número de

38. Descubierto en 2010, se desarrolló con el fin de sabotear las centrifugadoras utilizadas para el enriquecimiento de uranio en la planta nuclear iraní de Natanz. Entre la gran cantidad de información existente en la red al respecto, puede verse una muy sintética explicación del mismo en: *http://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra.*

grupos o entidades capaces de realizar este tipo de ciberoperaciones. Sin embargo, en el contexto de la llamada "Internet de las cosas", la omnipresencia de los ordenadores en muchas de los objetos que utilizamos en nuestra vida diaria hace que, prácticamente, cualquiera de ellos que esté equipado con un procesador sea susceptible de ser víctima de intrusiones y manipulaciones.

Cerraremos este apartado señalando que las operaciones de ciberseguridad estatales se dividen, básicamente, en cuatro áreas: Operaciones de Redes (*NetOps*), Operaciones de Ciberdefensa, Ataque de Redes Informáticas y Explotación de Redes Informáticas. Aunque la mayoría de las organizaciones estatales se centran principalmente en las dos primeras, las encargadas de la seguridad y la defensa nacional tratan de mantener la seguridad del ciberespacio también a través de la explotación y el ataque de redes y sistemas. Para entender lo que son unas y otras operaciones seguiremos el memorándum de la Junta de Jefes de Estado Mayor estadounidense, por el que se adoptó en 2010 la "terminología conjunta para las operaciones en el ciberespacio"[39].

Las Operaciones de Redes (*NetOps*) son las actividades conducidas para operar y defender la red de información global del Departamento de Defensa.

La Ciberdefensa es la aplicación integrada de las cibercapacidades del Departamento de Defensa u otros organismos gubernamentales y los procesos de sincronización en tiempo real de la capacidad de detectar, analizar y mitigar amenazas y vulnerabilidades, así como superar a los adversarios, con el objeto de defender redes específicas, proteger misiones críticas y permitir la libertad de acción.

La Explotación de Redes Informáticas se refiere a las capacidades relacionadas con la realización de operaciones facilitadoras y de recolección de información llevadas a cabo por medio de redes informáticas con el objeto de reunir datos acerca de los sistemas o redes objetivo.

El Ataque de Redes Informáticas se refiere, finalmente, a una categoría de acciones ofensivas realizadas a través de redes informáticas con el fin de perturbar, negar, degradar, manipular o destruir tanto la información albergada en sistemas o redes informáticas como los propios sistemas o redes.

Estos dos últimos tipos de ciberoperaciones son lo que en la (objeto de filtración) Directiva de Política Presidencial número 20[40] se definen,

39. *Joint Terminology for Cyberspace Operations* (2010). Accesible en: *http://www.nsciva.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.*

40. Hecha pública por WikiLeaks, la Directiva, emitida en 2012 con el título de *U.S. Cyber Operations Policy*, resulta accesible en: *http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.*

respectivamente, como operaciones de *Cyber Collection* y de *Cyber Effects.* Las primeras son aquellas operaciones y programas o actividades afines realizadas por o en nombre del Gobierno, en o a través del ciberespacio, con el objetivo principal de recopilar inteligencia –incluida la información susceptible de ser utilizada en operaciones futuras– de ordenadores o sistemas y redes de información y comunicación, con la intención de no ser detectados. Las segundas aluden, por su parte, a la manipulación, alteración, negación, degradación o destrucción de los equipos, sistemas de información o de comunicaciones, redes e infraestructura física o virtual controlada por ordenadores o sistemas de información, así como de la correspondiente información albergada en el ciberespacio.

## 2. EL DERECHO INTERNACIONAL DE LA CIBERSEGURIDAD

### 2.1. APLICACIÓN EN EL CIBERESPACIO DE LOS PRINCIPIOS GENERALES DEL DERECHO INTERNACIONAL PÚBLICO

Según nos explica Duncan B. Hollis[41], existen dos métodos predominantes cuando de lo que se trata es de regular jurídicamente el ciberespacio: a) la creación de normas específicamente adaptadas a las características del ciberespacio; b) la aplicación analógica al ciberespacio de normas jurídicas preexistentes. Uno y otro enfoque han sido utilizados a lo largo de los años en el ámbito interno. El Derecho Internacional, sin embargo, ha descansado casi enteramente en el método analógico a la hora de regular el ciberespacio, especialmente en los temas relativos al uso de la fuerza y al Derecho Internacional Humanitario.

Casi desde sus mismos orígenes, se ha reclamado para Internet un área jurídica propia (Derecho de Internet, Derecho de las nuevas tecnologías, Derecho del ciberespacio, Ciberderecho) con normas adaptadas a las especificidades de esta tecnología[42]. En el campo del Derecho internacional

41. Hollis, Duncan B. *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?,* en *Cyberwar: Law & Ethics for Virtual Conflicts* (J. Ohlin *et al*., eds., Oxford University Press, 2014); Temple University Beasly School of Law *Legal Studies Research Paper* nº 2014-16.

42. Hay, no obstante, autores que niegan radicalmente la existencia de esta nueva rama del Derecho. Entre ellos quizás el más famoso sea Frank H. Easterbrook, quien en una conferencia pronunciada en 1996, posteriormente publicada en el Foro Jurídico de la Universidad de Chicago con el título de *"Cyberspace and the Law of the Horse"* (El Ciberespacio y el Derecho del Caballo), argumentaba contra la idea de considerar al Ciberderecho como un sector específico en el campo de los estudios jurídicos. Easterbrook citaba a Gerhard Casper como autor de la expresión "Derecho del caballo", afirmando que los argumentos de Casper contra los estudios jurídicos especializados o de nicho eran igualmente aplicables a ese

no existe una rama especial para el ciberespacio ni tampoco normas específicas dedicadas al mismo dentro de las áreas tradicionales de aquél. La única excepción la constituye, como antes señalábamos, el Convenio de Budapest sobre la ciberdelincuencia de 2001. En el resto de las áreas, para la regulación del ciberespacio se ha debido, hasta ahora, recurrir al expediente de tomar préstamos de otros contextos por vía de la analogía.

De lo que se trata es, ante todo, de asegurar que el ciberespacio no es una zona inmune al Derecho. Es en este sentido, precisamente, en el que Marco Roscini[43] mantiene que la ausencia de reglas *ad hoc* no significa que las ciberoperaciones puedan ser conducidas por los Estados sin restricciones. Cita la opinión del Magistrado Simma acerca de que el punto de vista según el cual lo que no está expresamente prohibido se encuentra permitido refleja una visión anacrónica y sumamente consensualista del Derecho internacional, anclada en el principio elaborado por la Corte Permanente en el asunto del *Lotus*[44]. Por ello, dice Roscini, las normas internacionales convencionales y consuetudinarias pueden extenderse por vía interpretativa a las ciberoperaciones no expresamente contempladas en aquéllas.

Las ciberoperaciones equivalentes a un uso de la fuerza o a actos de hostilidades caerían de esta forma dentro de las áreas del Derecho internacional que regulan el derecho de los Estados al recurso a la fuerza (*ius ad bellum*) y la conducción de las hostilidades en caso de conflicto armado (*ius in bello*).

La reinterpretación de las disposiciones del *ius ad bellum* y del *ius in bello* para acomodarlas a la tecnología cibernética encuentra apoyo en el hecho de que no pocos Estados han declarado aplicables a la misma las normas preexistentes, incluyendo la Carta de las Naciones Unidas y el Derecho Internacional Humanitario. Así, por ejemplo, en 2011 la Casa Blanca emitió la Estrategia Internacional para el Ciberespacio[45], donde se señala

---

pretendido Ciberderecho: "[…] la mejor manera de encontrar el Derecho aplicable a los supuestos especializados es el estudio de las normas generales. Muchos casos tratan de la venta de caballos; otros se ocupan de las personas coceadas por caballos; otros versan acerca de la concesión de licencias y de las carreras de caballos, o con el régimen de los veterinarios que atienden a los caballos, o, en fin, con premios en espectáculos equinos. Cualquier esfuerzo por unificar todos estos flecos diversos en un curso sobre 'El Derecho del Caballo' está condenado a ser poco profundo y a perder sus principios unificadores".

43. *Op. cit.,* en nota 20.
44. Declaración del Magistrado Simma en la Opinión consultiva del Tribunal Internacional de Justicia de 22 de julio de 2010 sobre la *Conformidad con el Derecho internacional de la Declaración Unilateral de Independencia relativa a Kosovo.*
45. *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (2011). The White House. Washington.

que "el desarrollo de normas de conducta de los Estados en el ciberespacio no requiere de una reinvención del Derecho internacional consuetudinario, ni vuelve obsoletas las normas internacionales existentes. Las normas internacionales que desde hace mucho tiempo rigen el comportamiento de los Estados en tiempos de paz y de conflicto también se aplican en el ciberespacio". Además, en septiembre de 2012 el entonces Asesor Jurídico del Departamento de Estado, Harold KOH, dio un paso importante en la fijación pública de las posiciones estadounidenses sobre cómo el Derecho internacional se aplica al ciberespacio, durante una conferencia patrocinada por el Cibercomando de los Estados Unidos (USCYBERCOM)[46]. H. KOH afirmó en tal ocasión que los principios del derecho internacional se aplican en el ciberespacio, que éste no es una zona inmune al Derecho donde cualquiera pueda realizar actividades hostiles sin sujeción a reglas o restricciones, que en el contexto de un conflicto armado el Derecho de los conflictos armados regula el uso de las medios cibernéticos en las hostilidades, igual que sucede con otros medios de combate, y que los principios de necesidad y proporcionalidad limitan el uso de la fuerza en legítima defensa, regulando lo que constituye una respuesta adecuada en atención a las circunstancias.

Ya hemos visto también anteriormente que en la declaración formulada tras la cumbre de la OTAN celebrada en Cardiff (Gales) en septiembre de 2014 se dice de forma expresa que la política de la organización es reconocer que el Derecho Internacional, incluyendo la Carta de las Naciones Unidas y el Derecho Internacional Humanitario, se aplica en el ciberespacio. E, igualmente, por lo que a la actividad de las Naciones Unidas se refiere, en el Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional[47] presentado en junio de 2013, en el apartado correspondiente a "Recomendaciones sobre normas, reglas y principios de conducta estatal responsable", se señala, entre otras cosas, que:

– La aplicación de normas derivadas del Derecho internacional vigente que son pertinentes para el uso de las tecnologías de la información y las comunicaciones por los Estados es una medida fundamental con el fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales. Es necesario continuar realizando estudios para establecer un entendimiento común sobre cómo se aplicarán esas normas a la conducta

46. Véase el respecto el artículo de Michael N. SCHMITT "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" (2012). *Harvard International Law Journal,* vol. 54.

47. El grupo fue establecido en 2012 por la resolución 66/24 de la Asamblea General de las Naciones Unidas. El informe es accesible en español en: *http://www.un.org/es/comun/docs/index.asp?symbol=A%2F68%2F98&Submit=Buscar&Lang=S.*

estatal y el uso de las tecnologías de la información y las comunicaciones por los Estados. Dadas las singulares características de las tecnologías de la información y las comunicaciones, podrían elaborarse normas adicionales con el transcurso del tiempo.

– El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías.

– La soberanía de los Estados y las normas y principios internacionales que de ella emanan son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías que se halle en su territorio.

Si esto es así, tras este reconocimiento de que las normas del Derecho Internacional vigente son aplicables al ciberespacio, particularmente las que disciplinan el *ius ad bellum* y el *ius in bello,* la labor que inmediatamente a continuación ha de realizarse es la de determinar cómo se adaptan tales normas a las singularidades del ciberespacio. El esfuerzo más significativo que hasta la fecha se ha llevado a cabo a este respecto es el que ha plasmado en el conocido como Manual de Tallin sobre el Derecho internacional aplicable a la ciberguerra[48]. Fruto de un proyecto desarrollado a lo largo de tres años, en el que ha intervenido un grupo de reconocidos académicos y profesionales del Derecho internacional, el Manual de Tallin identifica el Derecho internacional aplicable a la ciberguerra estableciendo noventa y cinco reglas que rigen este tipo de conflictos. En el manual se abordan temas como la soberanía y la responsabilidad de los Estados en el ciberespacio (éstos, solo de forma muy somera), el *ius ad bellum*, el Derecho internacional humanitario y el Derecho de la neutralidad. Cada regla viene acompañada de un extenso comentario en el que se detallan las bases de cada una de ellas en los tratados y en el derecho consuetudinario, se explica cómo el Grupo de Expertos interpreta las normas aplicables en el contexto ciberespacial y se esbozan los desacuerdos dentro del grupo en cuanto a la aplicación de cada regla. El proyecto, dirigido por el profesor Michael N. Schmitt, Director del Departamento de Derecho Internacional de la Escuela de Guerra Naval de los Estados Unidos, se ha realizado por invitación del Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN, con sede en Tallin (Estonia).

Pese a que el Manual de Tallin cubre un amplio espectro de temas, deja fuera de forma deliberada una buena parte de ciberactividades. En su

48. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013). Cambridge University Press.

apartado introductorio se aclara, en este sentido, que el mismo no alcanza a toda aquella ciberactividad que se desarrolla por debajo del umbral del "uso de la fuerza", tal como esta expresión es entendida en el *ius ad bellum*. Queda, por tanto, fuera del Manual todo lo relativo a la cibercriminalidad y, por supuesto, la actividad relacionada con otras áreas del Derecho internacional tales como las relativas a los derechos humanos o al derecho de las telecomunicaciones. El Manual no es, en definitiva, un manual de Derecho internacional de la ciberseguridad, por lo que, por mucho que puedan representar serias amenazas para los Estados, las corporaciones y los individuos, el ciberespionaje, el robo de propiedad intelectual y una variada panoplia de actividades criminales en el ciberespacio no son objeto de tratamiento en aquél, por cuanto las normas de Derecho internacional sobre el uso de la fuerza y sobre los conflictos armados no juegan papel alguno con respecto a dichas actividades. Originalmente, pues, el Manual de Tallin se ha centrado en exclusiva en las ciberoperaciones más perjudiciales y destructivas, es decir, a las que cabe calificar como "ataques armados" y que, por tanto, permiten a los Estados responder en legítima defensa, así como en las que tienen lugar en el curso de conflictos armados.

En la página web del NATO CCD COE se nos anuncia, precisamente, la futura publicación en 2016 de una segunda edición del Manual, fruto de un proyecto actualmente en curso (Tallinn 2.0)[49], dirigido a ampliar el alcance del manual original. Reconociéndose que los Estados tienen el reto diario de hacer frente a ciberoperaciones malévolas que no llegan a los niveles antes mencionados, el proyecto Tallinn 2.0 examina el marco jurídico internacional que se aplica a este otro tipo de ciberoperaciones. Este futuro Manual de Tallin, de alcance más ambicioso, cubrirá, por tanto, las áreas del Derecho internacional relacionadas con la responsabilidad del Estado, el derecho del mar, el derecho internacional de las telecomunicaciones, el derecho espacial, el derecho diplomático y consular, y, con respecto a los individuos, las normas de derechos humanos. Tallinn 2.0 también explorará cómo se aplican en el ciberespacio ciertos principios generales del derecho internacional: soberanía, jurisdicción, diligencia debida y prohibición de la intervención. Materias todas ellas que, desde hace unos años, vienen siendo objeto de atención académica.

Concluiremos este apartado reconociendo con Michael N. Schmitt y Liis Vihul[50] que el derecho convencional ciber-específico es escaso y que hay un vacío casi total de derecho consuetudinario al respecto. Como resultado, no queda sino recurrir al Derecho internacional general. Si cualquier

49. Véase: *http://ccdcoe.org/research.html*.
50. Schmitt, Michael N. y Vihul, Liis. *The Nature of International Law Cyber Norms* (2014). NATO CCD COE Tallinn Paper nº 5.

esfuerzo interpretativo está de por sí plagado de incertidumbre y ambigüedad, ello es especialmente cierto cuando se realiza con respecto a actividades tan novedosas como las ciberoperaciones. A pesar de la atención prestada a las ciberactividades en la última década, la celebración de nuevos tratados o la cristalización de nuevas normas de derecho consuetudinario para gobernar aquéllas no parece que, por el momento, vaya a producirse. La oposición de los Estados occidentales es particularmente intensa, al menos en cuanto a la primera. En su lugar, la aplicación y la evolución interpretativa del Derecho internacional vigente es la más probable perspectiva a corto plazo. En cuanto al derecho consuetudinario, aunque a veces puede desarrollarse rápidamente, por regla general es demasiado lento como medio para adaptar la norma a circunstancias rápidamente cambiantes.

## 2.2. SOBERANÍA TERRITORIAL, DILIGENCIA DEBIDA Y NO INTERVENCIÓN EN EL CIBERESPACIO

Max Huber, en el laudo arbitral dictado en 1928 en el caso de la *Isla de Palmas*[51], afirmó que la soberanía en las relaciones entre los Estados significa independencia y que ésta es el derecho a ejercer sobre una porción del globo las funciones estatales, con exclusión de cualquier otro Estado. La soberanía territorial es, pues, ante todo un derecho, que conlleva simultáneamente un deber para el Estado, que es el de proteger en su territorio los derechos de los demás Estados. No es, por lo tanto, extraño que el Tribunal Internacional de Justicia proclamara que el respeto a la soberanía territorial constituye una de las bases esenciales sobre las que se asientan las relaciones internacionales[52].

Superadas por la realidad las tesis iniciales que conceptuaban al ciberespacio como un ámbito inmune a la soberanía estatal, su naturaleza de "dominio global" ha llevado, no obstante, a que algunos autores sugieran que debe dotarse al mismo de un estatus jurídico especial. Sean Kanuck[53] ha puesto de relieve que el hecho de que el ciberespacio se haya convertido en un elemento crítico de la sociedad moderna, donde se manifiesta la profunda interdependencia de todas las naciones, ha conducido a que algunos comentaristas estén considerando si este nuevo entorno tiene que ser considerado un *global commons*, un bien comunal global, que –al modo de la alta mar, la Antártida o el espacio exterior– deba ser gobernado colectivamente en beneficio común de toda la humanidad. Existen, no obstante, serias objeciones a esa consideración del ciberespacio como un *global*

51. Accesible en: *http://legal.un.org/riaa/cases/vol_II/829-871.pdf*.
52. Caso del *Canal de Corfú* (1949).
53. Kanuck, Sean. *Sovereign Discourse on Cyber Conflict Under International Law* (2010). Texas Law Review, vol. 88, pp. 1571 y ss.

*commons.* En primer lugar, en el ciberespacio no se produce esa "tragedia comunal" a que se refirió Garret HARDIN[54], conforme a la cual el uso indiscriminado de un recurso común llevará inevitablemente a que a largo plazo ese recurso se vea esquilmado o degradado. En segundo lugar, un régimen de *global commons* reclamaría la existencia de unas reglas comunes, que sería extremadamente difícil hacer cumplir dados los problemas de identificación y de atribución que, hoy por hoy, plantea el ciberespacio. Por último, la infraestructura del ciberespacio está sujeta a propiedad privada, por lo que el establecimiento de un régimen de *global commons* obligaría a realizar expropiaciones a gran escala, al tiempo que, por lo que a la regulación del acceso respecta, la identificación y consiguiente exclusión de usuarios ilegítimos es técnicamente complicada.

Lo cierto es que, como señala Wolff HEINTSCHEL VON HEINEEG[55], la práctica estatal nos ha dado buena muestra de que el ciberespacio o, mejor dicho, sus componentes, no son en modo alguno inmunes a la soberanía y al ejercicio de la correspondiente jurisdicción. Por una parte, los Estados ejercen y seguirán ejerciendo su jurisdicción en el orden penal con relación a los ciberdelitos. Por otra parte, debe recordarse que, como vimos, el ciberespacio requiere de una arquitectura física para existir. La integración en el dominio global del ciberespacio de esos componentes físicos situados en el territorio de los diversos Estados no puede, por consiguiente, interpretarse como una renuncia el ejercicio de la soberanía territorial. La aplicación del principio de soberanía a tales componentes, así como a las ciberactividades, no se ve, en suma, impedida por el carácter novedoso de la tecnología que le sirve de sustrato.

Una primera consecuencia de ello, dice HEINTSCHEL VON HEINEGG, es que las ciberinfraestructuras ubicadas en zonas bajo soberanía territorial están protegidas contra la injerencia de otros Estados. Protección que no se limita a las actividades que alcancen el nivel de un uso injustificado de la fuerza, un ataque armado o una intervención prohibida. Si la interferencia resulta en la producción de daños materiales a ciberinfraestructuras situadas en otro Estado, parece existir consenso suficiente acerca de que tal interferencia constituye una violación de la soberanía territorial del Estado donde aquélla se ha producido. Si no hay daños materiales o si éstos son leves, hay cierto debate doctrinal sobre si la intrusión puede ser considerada como una violación de la soberanía territorial. El ejemplo habitualmente citado es el del

54. HARDIN, Garret. *The Tragedy of the Commons*. Science, v. 162 (1968), pp. 1243-1248. Una traducción del artículo al español puede verse en: *https://www.uam.es/personal_pdi/ciencias/jonate/Eco_Rec/Intro/La_tragedia_de_los_comunes.pdf*.

55. HEINTSCHEL VON HEINEEG, Wolff. *Legal Implications of Territorial Sovereignty in Cyberspace* (2012). 4th International Conference on Cyber Conflict. C. CZOSSECK, R. OTTIS, K., ZIOLKOWSKI (Eds.). NATO CCD COE Publications.

espionaje, incluyendo el ciberespionaje, ya que, como más adelante se verá, el Derecho internacional carece de una prohibición del mismo. El hecho de que los datos albergados en el sistema objetivo se modifiquen por el acto de intrusión no parece, en principio, revestir suficiente entidad como para calificar dicho acto como violación del principio de soberanía territorial. Podría, sin embargo, argumentarse que la entidad del daño es irrelevante y que el mero hecho de que órganos de un Estado extranjero se hayan inmiscuido en la ciberinfraestructura de otro Estado debe ser considerado un ejercicio de la jurisdicción en territorio extranjero, lo que siempre constituirá una violación del principio de soberanía territorial.

La segunda consecuencia, según Heintschel von Heinegg, de la aplicabilidad del principio de soberanía territorial al ciberespacio es el amplio derecho del Estado territorial (incluidos el Estado de pabellón y el Estado de matrícula) para ejercer su jurisdicción tanto sobre ciberinfraestructuras como sobre ciberactividades. Las tres primeras reglas del Manual de Tallin se refieren, precisamente, a este aspecto de la soberanía:

– Conforme a la regla 1, relativa a la "soberanía", los Estados pueden ejercer control sobre las ciberinfraestructuras y ciberactividades dentro de su territorio soberano, lo que, entre otras cosas, significa que las mismas se encuentran sujetas a los poderes regulatorio, coercitivo y judicial del Estado soberano.

– De acuerdo con la regla 2, sobre "jurisdicción", sin perjuicio de las pertinentes obligaciones internacionales, los Estados pueden ejercer su jurisdicción: a) sobre las personas que realizan ciberactividades en su territorio; b) sobre las ciberinfraestructuras situadas en su territorio; c) extraterritorialmente, de conformidad con el Derecho internacional. La jurisdicción territorial puede ser objetivamente atribuida en relación con ciberactividades cuyos efectos se produzcan en un Estado aunque las mismas provengan de fuera de su territorio. Se citan en el Manual los ejemplos de las ciberoperaciones dirigidas desde fuera de su territorio contra Estonia en 2007 y contra Georgia en 2008[56], en los que la violación de las leyes estonias y georgianas que supusieron las interferencias producidas en el sistema bancario, en las funciones gubernamentales o en los medios de comunicación serían título habilitante para el ejercicio de sus respectivas jurisdicciones contra quienes perpetraron los ataques.

56. Un detallado estudio sobre estos ciberataques es el realizado por Nestor Ganuza Artiles en el capítulo cuarto, *Situación de la ciberseguridad en el ámbito internacional y en la OTAN*, del Cuaderno de Estrategia 149 (diciembre 2010) del Instituto Español de Estudios Estratégicos, titulado *"Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio"*.

– Según la regla 3, relativa a la "jurisdicción de los Estados de pabellón y de matrícula", las ciberinfraestructuras situadas a bordo de aeronaves, buques u otras plataformas en el espacio aéreo internacional, en la alta mar o en el espacio exterior se encuentran sujetas a la jurisdicción del Estado de pabellón o de matrícula.

Por otra parte, dado su carácter básico, el principio de soberanía territorial conlleva, como señalábamos al principio de este apartado, la obligación de todos los Estados de respetar la soberanía de los demás Estados. Esta obligación implica, según hizo notar el Tribunal Internacional de Justicia en el caso del *Canal de Corfú* (1949), que un Estado no debe permitir conscientemente que su territorio sea utilizado para realizar actos contrarios a los derechos de los demás Estados. Obligación esta que no se limita en exclusiva a la evitación de actos criminales, sino que se extiende también a todas las actividades susceptibles de causar serios daños a las personas u objetos situados en el territorio del otro Estado. En el célebre caso de la *Trail Smelter*, relacionado con un supuesto de polución ambiental transfronteriza, el laudo de la comisión arbitral de 1941 estableció que, de acuerdo con los principios del Derecho internacional, ningún Estado tiene el derecho de usar o permitir el uso de su territorio de tal manera que se cause daño en o al territorio de otro Estado o a las propiedades o personas en éste, con consecuencias graves.

Aplicando este deber de prevención al ciberespacio, la regla 4 del Manual de Tallin señala que "un Estado no debe permitir conscientemente que las ciberinfraestructuras situadas en su territorio o bajo su exclusivo control gubernamental sean usadas para realizar actos que afecten adversa e ilegalmente a otros Estados". La regla se aplica cuando el Estado tiene conocimiento efectivo de los actos en cuestión, esto es, cuando, por ejemplo, órganos estatales tales como los servicios de inteligencia han detectado o recibido información acerca de un ciberataque con origen en su territorio.

En lo que el grupo de expertos que elaboraron el Manual no consiguió alcanzar el consenso es en si la regla se aplica también al supuesto en que el Estado no tiene conocimiento de los actos pero podría haber adoptado medidas para tenerlo. Es, en efecto, difícil de determinar si un Estado ha violado el deber de prevención cuando no ha adoptado todas las posibles medidas de diligencia debida en el control de las ciberactividades desarrolladas en su territorio, habida cuenta de la facilidad con que los ciberatacantes pueden eludir dicho control. Hay, no obstante, en la doctrina quienes, como Matthew J. Sklerov[57], mantienen que los Estados que no

57. Sklerov, Matthew J., *Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent* (2009). Military Law Review, vol. 201, pp. 1 a 85.

promulguen leyes penales estrictas y establezcan medidas vigoras para su aplicación no cumplen con su deber de prevenir los ciberataques, de modo que si la pasividad y la indiferencia de ese Estado hacia los ciberataques llevan a que su territorio se convierta en un santuario desde donde los atacantes pueden operar con seguridad, dicho Estado puede ser considerado responsable indirecto de los ciberataques. Opina, sin embargo, HEINTSCHEL VON HEINEGG que la mera posibilidad teórica de que un Estado que no haya promulgado leyes penales, sin estar obligado a hacerlo en virtud de un tratado internacional, se convierta en un santuario para los ciberatacantes, no es ciertamente base suficiente para justificar la aplicabilidad del deber de prevención. Lo que le lleva a sugerir que, en lugar de tal presunción general, podría aplicarse una presunción de alcance más limitado en lo que se refiere a ese conocimiento estatal, en aquellas situaciones en que los ciberataques sean lanzados desde ciberinfraestructuras que se encuentran bajo exclusivo control gubernamental y que son usadas solo para fines no comerciales. Esto no significa, sin embargo, que la conducta pueda, sin más, ser atribuida a ese Estado, de forma que quepa recurrir al uso de contramedidas, ya que en el ciberespacio un enfoque de este tipo podría conducir a una escalada de tensión e imponer a los Estados obligaciones excesivamente estrictas, por cuanto esa ciberinfraestructura gubernamental bien pudiera haber sido tomada bajo control por otros Estados e, incluso, por actores no estatales, como terroristas o criminales.

Benedikt PIRKER[58] nos recuerda, por su parte, que el estándar de la diligencia debida está ampliamente aceptado en el campo de la prevención de los daños transfronterizos en el Derecho internacional del medio ambiente, por lo que cabe pensar que resulta asimismo aplicable a otras posibles violaciones de obligaciones internacionales y a otros daños diferentes. Los pasos que un Estado puede estar obligado a dar en una situación particular están determinados por el concepto de la "razonabilidad". Si, por ejemplo, continúa PIRKER, un Estado tiene conocimiento de que se está preparando un ciberataque dañino, entre las respuestas razonables podría estar la de aislar la red en cuestión.

En definitiva, a lo que el deber de prevención obliga, según Katharina ZIOLKOWSKI[59], es a que los Estados lleven a cabo una evaluación de riesgos y a informar, notificar y consultar a otros Estados en casos concretos de riesgo de daño transfronterizo significativo. Esto presupone la capacidad

58. PIRKER, Benedikt. *Territorial Sovereignty and Integrity and the Challenges of Cyberspace* (2013). Capítulo de la obra colectiva, editada por Katharina ZIOLKOWSKI, *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, publicada por el NATO CCD COE.

59. ZIOLKOWSKI, Katharina. *General Principles of International Law as Applicable in Cyberspace* (2013). Capítulo de la obra colectiva citada en la nota anterior.

de los Estados para detectar los flujos irregulares de datos o el software malicioso, lo que implica, al menos, la obligación de garantizar: 1º) Que los proveedores de Internet nacionales instalan sensores de red que recojan información sobre el flujo de red, es decir, sobre cantidad de datos enrutados y su destino (que permite la detección de, por ejemplo, ataques DDoS); 2º) Que los proveedores de Internet nacionales de nivel 1 instalan sistemas de detección/prevención de intrusión en sus "puertas" de transmisión internacional de datos y realizan un filtrado de paquetes profundo (que permita el reconocimiento de software malicioso), y 3º) Que existe un sistema de notificación obligatoria a una entidad gubernamental (por ejemplo, un CERT gubernamental) con respecto a los incidentes cibernéticos que se produzcan. Además, el deber de observar la diligencia debida también obligaría a los Estados a establecer cibercapacidades de investigación (que permitan identificar la fuente de las ciberactividades maliciosas), ya sea dentro de un CERT o de la policía u otras fuerzas de seguridad, en función de la distribución de responsabilidades establecida en las respectivas leyes nacionales, así como el marco institucional y jurídico que permita la prevención o la interrupción de concretas ciberactividades maliciosas que se originen en el territorio del Estado, susceptibles de perjudicar los derechos de otros Estados.

Otro principio derivado de la igualdad soberana de los Estados es el de no intervención en los asuntos domésticos de otro Estado, confirmado por el tribunal Internacional de Justicia como costumbre internacional. La esencia de lo que constituye intervención ilegal es razonablemente clara. Incluye acciones destinadas a coaccionar a un Estado para que realice o se abstenga de realizar algo a lo que tiene derecho conforme al Derecho internacional.

La ciberintervención sería, entones, una violación del principio de no intervención llevada a cabo en su totalidad, o al menos predominantemente, en el ciberespacio. En consecuencia, debe alcanzar ese nivel de actividad coercitiva ilegal con la que se trata de impedir que un Estado conduzca sus asuntos internos y sus relaciones exteriores de conformidad con sus propias decisiones dentro de los límites impuestos por el Derecho internacional.

Como señala Terry D. Gill[60], la ciberintervención, como su contraparte física, podría adoptar diversas formas y alcanzar distintos grados de intensidad. Incluiría formas variadas de desinformación y propaganda dirigidas a socavar la legitimidad de un gobierno extranjero, incitando a realizar actividades subversivas con el fin de agravar disturbios civiles

60. Gill, Terry D., *Non-Intervention in the Cyber Context* (2013). Capítulo de la misma obra colectiva citada en las notas anteriores.

o, incluso, derrocar a ese gobierno. El mal uso de las redes sociales, del correo electrónico y de las comunicaciones telefónicas digitales para tales fines podría ser un instrumento potencialmente poderoso en orden a incitar o ayudar a la oposición a un gobierno extranjero hostil. Podrían utilizarse también para manipular o influir en el resultado de las elecciones llevadas a cabo a través de procedimientos de votación digitales o para entrar en sitios web gubernamentales sensibles con el propósito de interferir con las comunicaciones gubernamentales o manipular actividades económicas y financieras. Tales actividades podrían debilitar la confianza en la capacidad del gobierno para mantener los servicios esenciales, la estabilidad económica y el orden público. Ataques coordinados de denegación de servicio a gran escala (DDoS) en sitios web económicos o financieros clave podrían dificultar o, incluso, paralizar la actividad gubernamental por cierto tiempo.

La ciberintervención también podría alcanzar un nivel en el que se llegara a sabotear instalaciones críticas, como una red de comunicaciones de defensa, un centro de investigación nuclear o un determinado sistema de armas, casos en los que podría estar cruzándose el umbral del uso de la fuerza hasta, incluso, equivaler a un ataque armado.

Algunas de estas actividades ya se han producido de hecho, como los ataques DDoS a Estonia en 2007 que, de probarse que estaban controlados o dirigidos por un Estado, habrían sido un caso claro de intervención prohibida por debajo de la umbral del uso de la fuerza. Otro ejemplo, al que ya nos hemos referido anteriormente, es el del "*Stuxnet*", que resultó en daños físicos limitados a centrifugadoras nucleares iraníes y que, al parecer, retrasó el desarrollo del programa de investigación nuclear de Irán durante cierto tiempo.

### 2.3. CONTRAMEDIDAS Y ESTADO DE NECESIDAD EN EL CIBERESPACIO

Un Estado víctima de una intervención ilegítima de otro Estado por debajo del umbral del uso de la fuerza puede responder por medio de contramedidas. En el artículo 22 del Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos[61] se establece que "la ilicitud del hecho de un Estado que no esté en conformidad con una obligación internacional suya para con otro Estado queda excluida en el caso y en la medida en que ese hecho constituya una contramedida tomada contra ese otro Estado".

61. Elaborado por la Comisión de Derecho Internacional, figura como anexo a la Resolución 56/83 de la Asamblea General, de 28 de enero de 2002.

Las contramedidas, así concebidas, tienen dos funciones esenciales. Por un lado, actúan a modo de circunstancia eximente de la responsabilidad internacional del Estado que recurre a ellas en violación de una obligación internacional. Por otro lado, son un medio para activar la responsabilidad del Estado adversario al que, con la adopción de las mismas, se trata de inducir al cumplimiento de sus obligaciones.

En su traslación al ciberespacio, conforme a la regla 9 del Manual de Tallin, un Estado que haya sido lesionado por un acto internacionalmente ilícito puede recurrir al uso de contramedidas proporcionadas, incluyendo cibercontramedidas, contra el Estado responsable.

Las contramedidas operan, por tanto, de un modo similar al de la legítima defensa, estando reservadas para aquellas ocasiones en que, dada la inexistencia de un ataque armado, el recurso a la legítima defensa no es jurídicamente posible. A través de aquéllas, la protección frente a un ciberataque inminente o en curso se tratará de alcanzar por medio de unas herramientas ofensivas que conforman lo que se conoce como "ciberdefensa activa". Ésta es definida en el Manual de Tallin como "una medida proactiva para la detección u obtención de información en cuanto a una ciberintrusión, un ciberataque o una ciberoperación inminente, o para determinar el origen de una operación, que implica el lanzamiento de una ciberoperación anticipada, preventiva o de respuesta contra la fuente". De lo que, en definitiva, se trata es de inhabilitar la fuente de la que procede el ataque.

Dicen Robin Geiß y Henning Lahmann[62] que puede haber casos en los que sea factible la identificación del territorio de origen y, por lo tanto, el establecimiento de la responsabilidad por, al menos, la violación del deber de prevenir. Sin embargo, igual que sucede en la legítima defensa, también el empleo de contramedidas es estrictamente instrumental, por lo que no se permiten como medio para tomar represalias y, en consecuencia, no son jurídicamente posibles una vez que el ciberataque ha cesado. Caso distinto es cuando un Estado no está enfrentándose a una intrusión aislada sino, más bien, a una cibercampaña maliciosa o a un ataque continuo pues, en este caso las contramedidas podrían ser herramientas de ciberseguridad útiles.

Por otra parte, señalan los citados autores que las defensas activas implican el empleo de un código potencialmente dañino dirigido al atacante o, incluso, la simple devolución de datos maliciosos hacia su fuente

62. Geiß, Robin y Lahmann, Henning. *Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention* (2013). Capítulo de la obra colectiva, editada por Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, publicada por el NATO CCD COE.

*(hack back)*, acción que podría dar lugar a una propagación incontrolable de códigos maliciosos que pongan en peligro a terceros previamente no involucrados. En opinión de la Comisión de Derecho Internacional, el hecho de que afecte a terceros no convierte *per se* a una contramedida en ilegal. Aunque esté claro que las contramedidas no pueden estar dirigidas contra Estados distintos del Estado responsable, esto no significa que no puedan afectar incidentalmente a terceros Estados o, incluso, a otros terceros, como inevitables efectos indirectos o colaterales. Ello no quiere decir que el Estado que recurre a contramedidas no deba tomar todas las medidas posibles para evitar afectar terceros o, si la lesión es inevitable, para asegurar que el impacto sea el mínimo posible. Cabe, entonces, preguntarse sobre el grado de diligencia debida que debe observar el Estado que recurre a las defensas activas como contramedidas contra un ciberataque. Según los autores citados, en aquellas situaciones en las que un Estado es consciente del hecho de que las medidas de ciberdefensa activa no pueden diseñarse de modo que no pueda evitarse que se extiendan sin control en los sistemas de terceras partes inocentes, causando pérdidas materiales, la respuesta debe considerarse ilegal en relación con el tercer Estado, dando origen a responsabilidad internacional.

Por otra parte, en el artículo 50 del Proyecto de artículos sobre responsabilidad del Estado se dispone claramente que la adopción de contramedidas no puede afectar a las obligaciones relativas a la protección de los derechos humanos fundamentales. Cabe, entonces, preguntarse si ciertas medidas de ciberdefensa activa podrían ser diseñadas de tal manera que se evitara una ejecución automática de las mismas, con riesgo de perjudicar seriamente derechos fundamentales debido a la muy alta probabilidad de propagación sin control. Se ha señalado que, por ejemplo, la sencilla devolución de un ataque DDoS es difícilmente controlable de tal modo que pueda minimizarse la causación de graves riesgos para la infraestructura civil en el país contra el que se dirigen las medidas. Como consecuencia de ello, parece dudoso que tal conducta nunca puede cumplir con el requisito del artículo 50 del Proyecto.

Otra cuestión especialmente crítica que los citados autores plantean en relación con el empleo de medidas de ciberdefensa activa como contramedidas es la relativa a la proporcionalidad. Por mucho que las defensas activas sean contramedidas recíprocas, lo que no está garantizado es que las mismas vayan a producir un efecto recíproco, ya que no se trata aquí de valorar la proporcionalidad en términos puramente cuantitativos. El juicio de proporcionalidad debe atender también a consideraciones cualitativas, en la medida en que el empleo de las medidas de defensa activa pueden dar lugar a resultados desproporcionados cuando se dirigen

contra infraestructuras críticas en el Estado de destino, pudiendo, en el peor de los casos, llegar a producir bajas civiles.

En cuanto a la reversibilidad de las contramedidas, exigida por el Proyecto de artículos[63], de la misma parece seguirse que medidas de ciberdefensa activa muy agresivas, destinadas, por ejemplo, a dañar un sistema para que deje de lanzar ataques futuros parece que serían difícilmente justificables. Tal conducta podría estar justificada en situaciones de legítima defensa, pero el requisito de reversibilidad impediría una justificación como contramedida. En el comentario a la regla 9 del Manual Tallin se señala a este respecto que, en el ámbito del ciberespacio, las acciones que impliquen la inhabilitación permanente de funciones cibernéticas no deben llevarse a cabo en aquellas circunstancias en que su interrupción temporal sea técnicamente factible y con ella se lograría el efecto necesario.

Distintas de las contramedidas son las acciones que un Estado puede adoptar sobre la base de un estado de necesidad. A éste se refiere el artículo 25 del Proyecto de artículos como causa de exclusión de la ilicitud de un hecho que no esté de conformidad con una obligación internacional, cuando tal hecho sea el único modo para el Estado de salvaguardar un interés esencial contra un peligro grave a inminente y el mismo no afecte gravemente a un interés esencial del Estado o de los Estados con relación a los cuales existe la obligación, o de la comunidad internacional en su conjunto.

El estado de necesidad sólo puede invocarse en circunstancias absolutamente excepcionales. Los requisitos para que su invocación pueda ser aceptada son, en consecuencia, muy estrictos. Trasladando esos requisitos al contexto ciber, parece razonable asumir que, cuando menos, la protección de las infraestructuras críticas sería aceptada como un interés esencial, y en esta dirección apuntan, precisamente, las declaraciones de varios Estados y organizaciones internacionales. Conceptuadas como estructuras indispensables para las funciones vitales de la sociedad, prácticamente todas las estrategias de ciberseguridad nacionales subrayan la protección de las infraestructuras críticas como uno de sus principales objetivos[64]. En este sentido, en el Manual de Tallin estos activos aparecen directamente vinculados a la noción de estado de necesidad, al afirmarse que, cuando se trata de hacer frente a importantes ciberoperaciones

63. En el artículo 49.3 del Proyecto se dispone que, en lo posible, las contramedidas serán tomadas en forma que permitan la reanudación del cumplimiento de las obligaciones que temporalmente incumple el Estado que recurre a ellas.

64. Así lo hace nuestra Estrategia de Ciberseguridad nacional de 2013, cuyo Objetivo II es el de "Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular".

contra sus infraestructuras críticas, los Estados pueden invocar el estado de necesidad para justificar el recurso a medidas dirigidas a contrarrestar dichas ciberoperaciones.

Señalan Robin Geiß & Henning Lahmann[65] que, en última instancia, el análisis del estado de necesidad desde el punto de vista de la ciberseguridad deja una impresión mixta. Mientras que, por una parte, a diferencia de lo que sucede con la legítima defensa y las contramedidas, las cuestiones relacionadas con la identificación y atribución pueden ser eludidas en este tipo de situaciones, las condiciones que se exigen en el artículo 25 del Proyecto de artículos son intencionadamente tan estrictas, que es muy dudoso que la ciberdefensa vía estado de necesidad pueda realizarse más que en unos pocos casos excepcionales. Por otra parte, precisamente porque no es precisa la atribución del acto para actuar contra sus potencialmente dañinos efectos, la doctrina alerta sobre posibilidad de que se cometan abusos graves, observación especialmente relevante si se tiene en cuenta que hay una persistente tendencia a tratar de justificar el uso de la fuerza invocando el estado de necesidad.

### 2.4. LA AMENAZA O EL USO DE LA FUERZA EN EL CIBERESPACIO. CIBERATAQUES ARMADOS Y DERECHO A LA LEGÍTIMA DEFENSA[66]

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

Es en la Carta de las Naciones Unidas de 1945, adoptada a la conclusión de la Segunda Guerra Mundial, cuando por vez primera en 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".*

65. *Op. cit.,* en nota 62.
66. Resumiré en este apartado lo que a este particular respecto desarrollé en un anterior trabajo, *"Ciberguerra y Derecho. El ius ad bellum y el ius in bello en el ciberespacio"*, publicado en el nº 100 de la Revista Española de Derecho Militar (2013).

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". Sintetizando la posición dominante, Katharina Ziolkowski[67] 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 ésta 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, 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*"[68].

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 aquélla.

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".*

Un aspecto en el que necesariamente debe repararse en la interpretación de este precepto es el relativo al 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

67. Ziolkowski, Katharina. *"Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt Criteria" for Use of Force"* (2012). NATO CCD COE Publications, Tallinn.

68. 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.

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 EEUU, no todo uso de la fuerza alcanza el nivel de ataque armado. Recuerda Nils MELZER[69] que, en el citado caso, el TIJ encontró necesario distinguir entre las más graves 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.

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.

### 2.4.1. 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[70], 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 TIJ, 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

69. MELZER, Nils. *"Cyberwarfare and International Law"* (2011). United Nations Institute for Disarmament Research (UNIDIR) Resources.

70. ROSCINI, Marco. *"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.

uso de la fuerza que se contienen en los artículos 2 (4), 51 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[71], 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 comunidad internacional entendería implican un uso de la fuerza. Michael SCHMITT, en su trabajo pionero de 1999[72], identificó un cierto número de factores, que el mismo autor ha vuelto a utilizar en un artículo más reciente[73], 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

71. *Op. cit.,* en nota 69.
72. SCHMITT Michael N., *"Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework". Columbia Journal of Transnational Law,* vol. 37, 1998-99, pp. 885 a 937.
73. SCHMITT, Michael. *"Cyber Operations and the Jus ad Bellum Revisited"* (2011). *Villanova Law Review*, 56, pp. 569-606.

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:

– *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.

– *Carácter militar:* La existencia de un nexo entre la ciberoperación en cuestión y la conducción de operaciones militares aumenta la probabilidad de que aquélla 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 ésta 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.

Tomando prestadas las palabras de Nils Melzer, 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).

### 2.4.2. Ciberataques armados

Según hemos visto, conforme a lo establecido en el art. 51 de la Carta de las Naciones Unidas, 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" implica necesariamente el uso de un arma. Ya hemos indicado anteriormente, sin embargo, que el TIJ 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), 51 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. Según la posición mayoritaria de la doctrina:

1º. 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.

2º. 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.

3º. 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 ya anteriormente referidas "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.

Por otra parte, como señala Michael N. SCHMITT, 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).

### 2.4.3. 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 éste, 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.

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.

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 embargo, una realidad, tal y como ha señalado Sean WATTS[74], 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[75] 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.

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.

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

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

74. WATTS, Sean. *"Low-Intensity Computer Network Attack and Self-Defense"* (2011). *International Legal Studies*, Vol. 87. US Naval War College.

75. 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).

necesidad, proporcionalidad, inminencia e inmediatez, cuyo juego en el ciberespacio determina, que:

1º. 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.

2º. La necesidad de la fuerza empleada debe relacionarse con la existencia o inexistencia de medios de acción alternativos que no impliquen el uso de aquélla. 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 ésta cinética o cibernética.

3º. 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.

4º. 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.

### 2.4.5. 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 es el Tratado del Atlántico Norte, firmado en Washington el 4 de abril de 1949. Por lo que respecta a la aplicación de su cláusula de defensa colectiva en el ciberespacio, en el Informe NATO 2020[76], 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 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. Así se ha reconocido, según ya hemos visto, en la nueva política que en materia de ciberdefensa se adoptó en la Cumbre de Gales celebrada en septiembre de 2014.

Ulf Häussler[77], 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

76. 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.*

77. Häussler, Ulf. *Cyber security and defence from the perspective of articles 4 and 5 of the NATO treaty*. Capítulo de la obra colectiva *"International Cyber Security Legal and Policy Proceedings"*, publicada por el NATO CCD COE (diciembre 2010).

lugar consultas y las capacidades para permitir una valoración militar de la situación estuvieron disponibles.

### 2.4.6. 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 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 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.

## 2.5. CIBERESPIONAJE Y DERECHO INTERNACIONAL: DEBATES ACTUALES

De todas las noticias que, prácticamente a diario, aparecen en los medios relacionadas con ciberactividades, son, sin duda, las que tienen que ver con el ciberespionaje las de mayor frecuencia. Sin ir más lejos, al tiempo de escribirse estas líneas nos hemos desayunado, en noviembre de 2014, con la información acerca de que la compañía Symantec ha detectado una avanzada herramienta de ciberespionaje que funciona desde 2008[78].

El ciberespionaje, también conocido como ciberexplotación, ha sido definido por Herbert S. Lin[79] como "el uso de acciones y operaciones –que pueden desarrollarse a lo largo de un período dilatado de tiempo– con el fin de obtener información que de otro modo se mantendría confidencial y que está albergada o en tránsito a través de sistemas o redes de ordenadores de un adversario".

Katharina Ziolkowski[80], a quien básicamente seguiremos en este apartado, propone una definición del ciberespionaje como "la copia de datos no accesibles al público, bien mientras se trasmiten por vía inalámbrica, bien mientras están guardados o temporalmente disponibles en sistemas o redes de ordenadores situados en el territorio o en un área bajo la jurisdicción exclusiva de un Estado, llevada a cabo por un órgano o agente de otro Estado, o de otra manera imputable a un Estado, en secreto, bajo disfraz o con falsas pretensiones, sin el consentimiento o aprobación de los

78. De nombre Regin, este *malware*, una vez instalado en un equipo, es capaz de hacer capturas de pantalla, robar contraseñas o recuperar archivos borrados, entre otras funcionalidades. Con un diseño muy adecuado para operaciones de vigilancia persistentes, su sofisticación ha llevado a pensar que en su desarrollo pudo haber participado un gobierno. *Vid.* la información al respecto en*: http://www.elmundo.es/tecnologia/2014/11/24/547301ab22601ddf7a8b457a.html*.

79. Lin, Herbert S., *Offensive Cyber Operations and the Use of Force* (2010). *Journal of National Security Law* & *Policy*, vol. 4, pp. 63 y ss.

80. Ziolkowski, Katharina. *Peacetime Cyber Espionage – New Tendencies in Public International Law* (2013). Capítulo de la obra colectiva, editada por Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, publicada por el NATO CCD COE.

propietarios u operadores de los sistemas o redes informáticas ni tampoco del Estado territorial".

Al ponerse el énfasis en el copiado de datos, se quiere significar que el ciberespionaje no afecta ni a la integridad ni a la disponibilidad de la información, sino tan solo a su confidencialidad. Por otra parte, esta segunda definición es más restrictiva que la primera en cuanto se limita al ciberespionaje conducido por Estados, omitiendo, por ejemplo, el que puedan llevar a cabo organizaciones internacionales.

En cuanto a la consideración jurídica que haya de darse al espionaje practicado en tiempo de paz, hay diferentes opiniones doctrinales. Algunos autores afirman que es ilegal; otros afirman que es legal, y la mayoría sostiene que el espionaje en tiempo de paz no es ni legal ni ilegal. Resumiremos a continuación estas diferentes posiciones tal como las expone la citada K. ZIOLKOWSKI.

1º. La ilegalidad del espionaje se ha basado en argumentos de diverso tipo. Algunos autores sugieren que esa ilegalidad procede del hecho de que el espionaje esté penalmente castigado en el Derecho interno de los diferentes Estados. Otros argumentan que el espionaje viola la integridad territorial o la independencia política de otros Estados. Se argumenta, asimismo, que el espionaje vulnera el principio de cooperación pacífica entre los Estados. Incluso hay autores que, expandiendo de manera incorrecta el concepto de espionaje para incluir dentro del mismo la denominada "acción encubierta", afirman que aquél viola el principio de no intervención.

2º. Por su parte, la legalidad del espionaje se ha defendido afirmando que el mismo es un componente de la legítima defensa anticipada o preventiva y que, por lo tanto, es un medio necesario para de la defensa del Estado[81]. También se ha defendido la legalidad del espionaje alegando que se trata de una práctica estatal ampliamente extendida, como lo prueba la existencia de servicios de inteligencia gubernamentales.

3º. La mayor parte de la doctrina entiende, sin embargo, que el Derecho internacional guarda silencio acerca de la legalidad o ilegalidad del espionaje estatal en tiempo de paz. El enfoque que el Derecho internacional clásico daría a una situación como esta sería el establecido en 1927 por el

81. Este argumento se apoya generalmente en el incidente ocurrido durante la Guerra Fría, en mayo de 1960, cuando un avión espía estadounidense U-2 fue derribado sobre la Unión Soviética. En un principio, el gobierno de Estados Unidos negó el objetivo y misión del avión, pero se vio obligado a admitir su papel en la intrusión aérea cuando la URSS mostró sus restos y anunció que su piloto, Francis Gary Powers, había sobrevivido a su derribo. El Secretario de Estado norteamericano justificó el espionaje diciendo que se trataba de una medida para disminuir y hacer frente al peligro de un ataque sorpresa.

Tribunal Permanente de Justicia Internacional en el caso del *Lotus*, al que ya nos hemos referido anteriormente. Con base en la noción de soberanía estatal, en ausencia de una prohibición legal, un Estado gozaría de una presunción *iuris tantum* de libertad de acción. Por el contrario, un enfoque iusinternacionalista consensual presume que, en caso de falta de regulación, nos hallamos ante una laguna jurídica de la que no puede derivar ningún permiso para actuar. La situación en cuestión tendría que considerarse simplemente como no regulada por el Derecho internacional (*non liquet*). Por lo tanto, caben dos opciones: o bien el espionaje estaría permitido, ya que no está prohibido (con base en la noción de soberanía estatal), o bien, como no está regulado, no podría ser objeto de enjuiciamiento conforme al Derecho internacional. En conclusión, los Estados son libres de realizar actividades extraterritoriales de ciberespionaje en tiempo de paz. Mientras que los medios utilizados para obtener acceso a los datos pueden violar el Derecho internacional, la copia de datos por sí sola no lo hace.

La emergencia del ciberespionaje parece, no obstante, estar dando lugar a un cambio de percepción, que lleva a considerarlo como algo relevante desde el punto de vista de la seguridad nacional. Ello, dice K. Ziolkowski, podría explicar recientes esfuerzos acometidos por algunos juristas, predominantemente de los Estados Unidos, para introducir nuevas interpretaciones en relación con el derecho a la legítima defensa en respuesta al ciberespionaje y con la noción de violación de la soberanía territorial vía ciber-intrusiones.

Hay autores que, en efecto, consideran las actividades de ciberespionaje como un "ataque armado", si manifiestan una intención hostil, la cual, dicen, debe presumirse en los casos de ciberespionaje contra sistemas informáticos sensibles, importantes para la defensa del Estado: sistemas de alerta temprana o de mando y control militar, sistemas informáticos de defensa de misiles, etc. Sin embargo, desde la propia Administración estadounidense se ha manifestado que el derecho a usar la fuerza en legítima defensa contra un ataque electrónico extranjero requiere que la conducta del intruso o el contexto de la actividad manifiesten claramente una intención maliciosa[82]. Es decir, que el aspecto decisivo es esta clara manifestación de la intención hostil, que permite suponer razonablemente que nos hallamos ante una situación de "inminente" ataque armado, activando el derecho a actuar en legítima defensa. Pero esta situación no puede darse en relación con el ciberespionaje, en primer lugar, porque las actividades de ciberespionaje son, por naturaleza, conducidas en secreto. Incluso si se descubren, ante los desafíos que presenta la atribución de las actividades

82. *An Assessment of International Legal Issues in Information Operations* (1999). Department of Defense Office of General Counsel.

*online*, ni la fuente de las mismas ni la intención de esa fuente desconocida o sólo supuesta puede ser evaluada con precisión hasta el punto de permitir la movilización de las fuerzas armadas propias y ejecutar medidas de defensa. Además, la intención de los actos de espionaje como tales no es más que la recopilación de información con objetivos que pueden carecer de carácter agresivo.

Por otro lado, el espionaje llevado a cabo dentro de las zonas bajo jurisdicción de otro Estado soberano –el territorio terrestre, las aguas interiores, el mar territorial, espacio aéreo nacional, etc.– tradicionalmente requiere la introducción clandestina y no autorizada de un agente de un Estado extranjero o de una plataforma de recogida de información, tal como un avión, un barco o un submarino. En tales casos, la soberanía territorial, es decir, el ejercicio de la autoridad plena y exclusiva sobre un territorio o área, sería violada. Sería también el caso del ciberespionaje por vía del denominado "acceso próximo" hacia sistemas o redes aisladas. En cuanto a las ciberactividades conducidas remotamente, es decir, que no requieren de la presencia física en zonas bajo la soberanía del Estado objetivo, es cuestionable, según K. Ziolkowski, que un mero "traspaso virtual no autorizado" pueda equipararse a la intrusión o presencia física en territorio extranjero. Sin embargo, algún un autor ha hecho notar que se podría argumentar que una intrusión en una infraestructura cibernética de un Estado por órganos o agentes de otro Estado debe considerarse como un ejercicio de jurisdicción en territorio extranjero, lo que siempre constituirá una violación del principio de soberanía territorial. Este punto de vista no se centra, pues, en el "traspaso virtual", sino en el ejercicio de la autoridad por un representante de un Estado extranjero.

Concluiremos este apartado con las palabras de K. Ziolkowski acerca del cambio de enfoque que ha tenido lugar en el análisis desde el Derecho internacional de las ciberactividades maliciosas. Señala esta autora que hace unos 15 años el discurso académico estaba centrado en torno a la distinción entre el "uso de la fuerza armada" y el "ataque armado" ilegales y las perfectamente legales medidas de coerción política o económica. El cambio recientemente perceptible en cuando al objeto de análisis, así como de las líneas de argumentación jurídica, podría estar fundado en la idea de que la satisfacción con el *statu quo* político ha cambiado muy probablemente con respecto al ciberespionaje. A diferencia de las circunstancias que concurren en el discurso sobre la coerción política o económica, los Estados económicamente y militarmente fuertes son los que tienen mucho más que perder, especialmente a través de ciberespionaje de motivación económica dirigido contra sus logros tecnológicos industriales y post-industriales, que puede menoscabar su ventaja competitiva, reduciendo su

posición ventajosa en el sistema globalizado de la economía mundial. En otras palabras, la ventaja asimétrica que ofrecen los medios cibernéticos puede contrarrestar mucho del poder convencional que poseen esos Estados. De ahí que entienda la citada autora que esos esfuerzos interpretativos encaminados a declarar fuera de la ley al ciberespionaje política o económicamente motivado, considerándolo un uso ilegal de la fuerza o un ataque armado, o bien una violación de la soberanía territorial, no persiguen otra cosa que preservar las ventajas estratégicas de las grandes potencias.

## 2.6. EL "IUS IN BELLO" EN EL CIBERESPACIO: IDEAS BÁSICAS[83]

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[84], "como un vasto conjunto normativo que persigue controlar jurídicamente el fenómeno bélico –reglamentando los métodos y medios de combate, distinguiendo entre personas y bienes civiles 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".

Las fuentes más importantes del DIH están constituidas por los cuatro Convenios de Ginebra de 12 de agosto de 1949[85], sus dos Protocolos Adicionales de 8 de junio de 1977[86], 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

83. Selección de los aspectos generales de lo que, a este particular respecto, desarrollé en *"Ciberguerra y Derecho. El ius ad bellum y el ius in bello en el ciberespacio"*, publicado en el nº 100 de la *Revista Española de Derecho Militar* (2013).

84. Pérez González, Manuel. *El Derecho Internacional Humanitario frente a la violencia bélica: una apuesta por la humanidad en situaciones de conflicto.* Capítulo 1 de la obra *"Derecho Internacional Humanitario"* (ed. 2007) del Centro de Estudios de Derecho Internacional Humanitario de Cruz Roja Española, publicada por Tirant lo Blanch.

85. 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.

86. 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.

convencionales, existe un *ius in bello* consuetudinario, que ha sido objeto de un laborioso estudio publicado por el Comité Internacional de la Cruz Roja[87], 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 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[88], 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 éste 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 causa-

87. *"Study on customary international humanitarian law: a contribution to the understanding and respect for the rule of law in armed conflict"* (2005). Autor: Jean-Marie Henckaerts.

88. *Op. cit.*, en nota 69.

ción 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 de 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. En cualquier caso, tanto el Manual de Tallin como Erki Kodar[89] recuerdan 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[90] 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.

En cuanto al concepto de "ciberataque" en el *ius in bello*, hay que tener en cuenta que 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, pues de ella depende la aplicación a las ciberoperaciones de las muy numerosas normas del DIH que regulan, limitándolos, los ataques.

89. Kodar, Erki. *Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I* (2012) ENDC Proceedings, vol. 15, 2012, pp. 107-132.
90. PA I, Artículo 1.2.

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[91], que el término "operaciones" que emplea el art. 48 del PA I determinaría 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 éstos son *"los actos de violencia contra el adversario, sean ofensivos o defensivos".*

Lo que con William H. Boothby[92] 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, ésta sea considerada como un "ciberataque" a los efectos de aplicación del DIH. Se dice, así, en el Manual de Tallin, que "un ciberataque es una ciberoperación, ofensiva o defensiva, de la que cabe razonablemente esperar que cause lesiones o muerte a las personas o daño o destrucción a los objetos". Y se pone como ejemplo el de una ciberoperación que alterara el funcionamiento del sistema SCADA[93] de una red

91. Schmitt, Michael N. *Cyber Operations and the Jus in Bello: Key Issues* (2011). International Law Studies, vol. 87. US Naval War College.
92. Boothby, William H. *The Law of Targeting* (2012). Oxford University Press. Capítulo 18, sobre *"Cyber Targeting".*
93. 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.

eléctrica provocando un grave incendio, cuyas consecuencias destructivas determinarían la consideración de aquélla 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[94] 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 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, 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

94. Dörmann, Knut. *The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint* (2004). Karyn Byström (Ed.). International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17-19 de noviembre de 2004. Estocolmo.

reinstalación del sistema operativo, también debe ser considerada como un ataque, al entender aquéllos 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[95]. El DIH se aplicaría, entonces, plenamente a tal tipo de ciberoperaciones.

## 3. RELACIONES INTERNACIONALES Y CIBERESPACIO: INICIATIVAS DE LA ASAMBLEA GENERAL DE LAS NACIONES UNIDAS

Al tiempo que Internet se ha convertido en una auténtica red global, indispensable para la vida social, política, económica y cultural de nuestras sociedades, tanto en los medios como en la doctrina especializada se nos viene alertando sobre una suerte de nueva guerra fría que se estaría desarrollando en el ciberespacio[96]. La ciberseguridad ha mutado, en consecuencia, como ya hemos señalado, de ser originalmente una disciplina puramente técnica a constituir una parte importante de las estrategias de seguridad nacionales. No en vano, se ha hablado de la posibilidad de que el ciberespacio se transforme en un campo de batalla global y, de hecho, en no pocos países se considera a aquél como el quinto ámbito de la guerra (los otros cuatro son el terrestre, el marítimo, el aéreo y el espacial).

Ya desde los años noventa del pasado siglo se viene hablando de alcanzar un acuerdo internacional para limitar el riesgo de que se produzca un ciberconflicto armado[97]. No obstante, no parece que a día de hoy pueda llegarse a un acuerdo de tales características, entre otras razones porque cualquier esfuerzo encaminado a eliminar o reducir el software malicioso no es factible, ya que, por una parte, su intangibilidad hace que no sea posible someter el mismo a mecanismos de control y verificación y, por

95. Fue el caso de la operación *Orchard* (septiembre de 2007), en la que el ataque de Israel contra un reactor nuclear sirio estuvo precedido por un ciberataque que cegó el sistema de defensa aérea de Siria.
96. Véase, por ejemplo, el trabajo de Eguskiñe Lejarza Illaro *"Estados Unidos-China: Equilibrio de poder en la nueva ciber guerra fría"*. Documento de opinión 60/2013 del Instituto Español de Estudios Estratégicos. Accesible en: *http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO60-2013_Ciberguerra_Fria_EEUU-China_E.Lejarza.pdf.*
97. En 1998 la Federación Rusa propuso un tratado dirigido a prohibir el uso del ciberespacio para fines militares.

otra, su código es difícilmente reconocible como malicioso sin un análisis profundo que, además, permita averiguar el uso que se pretende dar al mismo. Además, los Estados se muestran reacios a deshacerse de las posibilidades que ofrece la utilización no letal de las ciberarmas con fines de perturbación o interferencia.

Propuestas como la realizada en septiembre de 2011 por China, la Federación Rusa, Tayikistán y Uzbekistán, para que por medio de una resolución de la Asamblea General de las Naciones Unidas se adoptará un "Código Internacional de Conducta para la Seguridad de la Información", que incluyera medidas de no-proliferación, no han encontrado por el momento un terreno fértil donde poder fructificar. Entre otras razones, no es la menor la determinada por las diferencias terminológicas: mientras los Estados miembros de la Organización para la Cooperación de Shanghái utilizan la expresión "seguridad de la información", en los Estados occidentales se habla de "ciberseguridad", lo que, más allá de la pura diferencia nominal, refleja un diferente enfoque con relación al siempre complicado equilibrio entre la seguridad y las libertades civiles. En tanto unos Estados ponen el foco principalmente en el respeto a los principios de soberanía e integridad territorial, en la seguridad nacional y en la estabilidad política, otros subrayan la importancia de salvaguardar los derechos humanos y el libre flujo de información, así como de promover la cooperación policial y el intercambio de información.

No obstante, las diferencias de planteamiento que existen en la comunidad internacional en torno a cómo garantizar la seguridad en el ciberespacio no han impedido que se hayan emprendido ciertas iniciativas diplomáticas tendentes a la adopción de "medidas de fomento de la confianza" en este campo. Este tipo de medidas, como instrumento de las relaciones internacionales, fue desarrollado entre las alianzas militares durante la guerra fría con el fin de evitar ataques nucleares por accidente, y, a partir de entonces, su uso se ha ido extendiendo a otras áreas, tanto militares como no militares[98]. Como dice K. Ziolkowski[99], las directrices desarrolladas con relación a este tipo de medidas en el área del desarme son también adecuadas para su aplicación al ciberespacio, donde de lo que se trata es de, primero, conseguir una base de entendimiento mutuo acerca de lo que debe ser el comportamiento aceptable de los Estados en el

98. En cuanto a las relativas a las armas, véase la exposición contenida en la web de la UNODA, United Nations Office for Disarmament Affairs: *http://www.un.org/disarmament/convarms/infoCBM/*

99. Ziolkowski, Katharina. *Confidence Building Measures for Cyberspace* (2013). Capítulo de la obra colectiva, editada por Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, publicada por el NATO CCD COE.

ciberespacio y, después, alcanzar la estabilidad en las relaciones internacionales en dicho entorno.

Además de en la OSCE[100], las iniciativas más relevantes en este campo son las que están teniendo lugar en el marco de las Naciones Unidas, en cuya agenda está presente el tema de la ciberseguridad desde que en 1998 la Federación Rusa presentara un proyecto de resolución en la primera Comisión (Desarme y Seguridad Internacional) de la Asamblea General de las Naciones Unidas, que fue aprobada con el título de *"Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional"*[101]. A partir de este momento, las líneas de actuación que, en relación el ciberespacio, viene desarrollando la Asamblea General de las Naciones Unidas, están relacionadas con la actividad de esta primera Comisión, en la que centraremos nuestra atención, pero también con la de la segunda Comisión (Asuntos Financieros y Económicos) y con la de la tercera (Asuntos Sociales, Humanitarios y Culturales)[102].

100. La OSCE viene prestando gran atención a los temas relacionados con el fomento de la confianza en materia de ciberseguridad, como lo refleja la lectura de la resolución que sobre esta materia adoptó la Asamblea Parlamentaria en 2011, *"El enfoque general de la OSCE para fomentar la ciberseguridad"*, accesible en: *http://www.oscepa.org/publications/declarations/2011-belgrade-declaration/686-belgrade-resolutions-spanish/file.* Asimismo, en 2013 se ha adoptado por la Asamblea Parlamentaria de la OSCE una nueva resolución sobre *"La Ciberseguridad"*, en la que, tras lamentar que, hasta la fecha, la comunidad internacional no haya sido capaz de acordar medidas específicas para combatir las ciberamenazas, insta a los parlamentarios y las parlamentarias de los Estados participantes de la OSCE a intensificar sus esfuerzos para convencer al Parlamento y gobierno de su país de que las amenazas procedentes del ciberespacio constituyen uno de los desafíos más graves en materia de seguridad de nuestros días, y pueden poner en peligro la forma de vida de las sociedades modernas y la civilización en su conjunto. Esta última es accesible en: *http://www.oscepa.org/publications/declarations/2013-istanbul-declaration/1821-istanbul-declaration-spanish/file.*

101. A/RES/53/70, de 4 de enero de 1999, accesible en: *http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=S.*

102. En esta Comisión se presentó en noviembre de 2013 un proyecto de resolución sobre *"El derecho a la privacidad en la era digital"*, en el que tras señalarse que "observando que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad", se exhorta a todos los Estados a que, entre otros cosas, "examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del

Por lo que al trabajo de la primera Comisión se refiere, tras una propuesta rusa presentada en el año 2001, se constituyó un primer grupo de expertos gubernamentales (GEG) con el encargo de discutir sobre las amenazas, posibles vías de cooperación y otros aspectos relacionados con la seguridad internacional en el ámbito de la información y las telecomunicaciones. Este primer GEG, que trabajó entre 2004 y 2005, no llegó a emitir ningún informe, al no poder alcanzar un consenso. Sí que lo consiguió, por el contrario, un segundo GEG, que desarrolló sus trabajos entre 2009 y 2010, que presentó un informe[103] en el que se recomendaba la adopción de nuevas medidas para el fomento de la confianza y para reducir el riesgo de las percepciones erróneas resultantes de las perturbaciones de las tecnologías de la información y las comunicaciones, como, por ejemplo:

– Proseguir el diálogo entablado entre los Estados para examinar las normas relativas al uso de las tecnologías de la información y las comunicaciones por los Estados, reducir los riesgos colectivos y proteger los elementos esenciales de la infraestructura nacional e internacional;

–Adoptar medidas de fomento de la confianza, de estabilidad y de reducción de los riesgos para abordar las consecuencias del empleo de las tecnologías de la información y las comunicaciones por los Estados, incluidos los intercambios de las opiniones nacionales sobre el empleo de esas tecnologías en los conflictos;

–Intercambiar información sobre la legislación nacional y las estrategias y tecnologías, políticas y mejores prácticas nacionales en cuanto a la seguridad de las tecnologías de la información y de las comunicaciones.

El 2 de diciembre de 2011 la Asamblea General adoptó la Resolución nº 66/24, sobre *"Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional"*[104], en la que se solicitaba del

---

derecho internacional de los derechos humanos". Los promotores de este proyecto de resolución han sido, no por casualidad, Brasil y Alemania, primeras víctimas de las operaciones de vigilancia electrónica de la NSA de los Estados Unidos, conocidas por las relevaciones de E. Snowden. Anteriormente, en abril de 2013, se había presentado el informe de Frank La Rue, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, relativo a las implicaciones de la vigilancia de las comunicaciones realizada por los Estados en el ejercicio de los derechos humanos a la privacidad y a la libertad de opinión y expresión, el cual, entre sus recomendaciones incluye los estándares jurídicos a que deben estar sujetas esas medidas de vigilancia de las comunicaciones.

103. A/65/201, de 30 de julio de 2010, accesible en: *http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=S.*

104. A/RES/66/24, accesible en: *http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/66/24&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=S.*

Secretario General que, con la asistencia de un nuevo GEG, establecido en 2012 sobre la base de una distribución geográfica equitativa y teniendo en cuenta las evaluaciones y recomendaciones que figuran en el informe del previo GEG, continuara examinando las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza respecto del espacio informativo, y que en su sexagésimo octavo período de sesiones (2013) le presentara un informe sobre los resultados de dicho examen.

El informe de este tercer GEG[105] sobre los *"Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional"* fue elevado al Secretario General el 7 de junio de 2013. En el primer párrafo de su introducción se señala que el uso de las tecnologías de la información y las comunicaciones (TIC) ha transformado el entorno de la seguridad internacional; que estas tecnologías aportan unas ventajas económicas y sociales inmensas, pero también pueden utilizarse para fines contrarios a la paz y la seguridad internacionales, y que durante los últimos años se ha producido un aumento perceptible del uso de las tecnologías de la información y las comunicaciones con finalidades delictivas y de desestabilización.

Entre las amenazas, riesgos y aspectos vulnerables, que en dicho informe se mencionan, cabe destacar los relacionados con:

– Los grupos terroristas, que utilizan las TIC para comunicarse, recopilar información, reclutar adeptos, organizar, planificar y coordinar ataques, promover sus ideas y actividades, y recabar financiación.

– El uso creciente de las TIC en infraestructuras y sistemas de control industrial fundamentales, que genera nuevas posibilidades de desestabilización.

En dicho informe se formulan ciertas recomendaciones sobre normas, reglas y principios de conducta estatal responsable, comenzando por señalarse que la aplicación de normas derivadas del Derecho internacional vigente que son pertinentes para el uso de las TIC por los Estados es una medida fundamental con el fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales, así como también determinadas recomendaciones sobre medidas de fomento de la confianza y el intercambio de información.

105. A/68/98, accesible en: *http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/sgreports/68/&Lang=S.*

El informe termina concluyendo que el progreso en el ámbito de la seguridad internacional en el uso de las TIC por los Estados será iterativo: cada paso del camino partirá del anterior; y que este enfoque será necesario porque el entorno tecnológico está configurado por el cambio y por el crecimiento constante del número de usuarios de las tecnologías de la información y las comunicaciones.

El siguiente paso en ese camino, dentro la labor de la primera Comisión, fue el que llevó a la aprobación, el 27 de diciembre de 2013, de la Resolución 68/243 de la Asamblea General sobre *"Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional"*[106]. En ella se solicita al Secretario General que, con la asistencia de un cuarto GEG, teniendo en cuenta las evaluaciones y recomendaciones que figuran en el informe del anterior, continúe examinando, con miras a promover un entendimiento común, las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza, las cuestiones relativas al uso de las TIC en los conflictos y la manera en que se aplica el derecho internacional al uso de esas tecnologías por los Estados, y que en su septuagésimo período de sesiones (2015) le presente un informe sobre los resultados de dicho examen. Este cuarto GEG, compuesto de 20 expertos, ha celebrado su primera reunión en Nueva York, en julio de 2014.

En fin, el consenso alcanzado acerca de que el Derecho internacional, en particular los principios de la Carta de las Naciones Unidas, son aplicables a las actividades de los Estados en el ciberespacio, incluyendo las actividades de actores no estatales que son atribuibles a los estados, constituye un primer paso, que permitirá a la comunidad internacional y los Estados afectados reaccionar de manera más efectiva frente a las violación de las obligaciones internacionales. En el ciberespacio, como hemos visto, los Estados se encuentran sujetos a la prohibición de la amenaza o el uso de la fuerza y a la obligación de respetar la soberanía y la independencia territorial de los otros Estados, del mismo modo en que lo están en el mundo físico, en ese mundo "de carne y acero" del que hablaba Barlow. Esas medidas de fomento de la confianza y el intercambio de información entre los Estados serán, en el día a día, las vías esenciales para aumentar la previsibilidad y reducir los riesgos de que un error de percepción pueda conducir a una escalada de tensión en el ciberespacio.

106. A/RES/68/243, accesible en: *http://www.un.org/es/comun/docs/?symbol=A/RES/68/243.*