*Análisis GESI, 7/2015*

# Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario

Jesús Reguera Sánchez

*14 de junio de 2015*

En el principio de los tiempos fue la palabra, después la escritura, más tarde el papel y así sucesivamente se ha llegado a los ordenadores y a su interconexión en el ciberespacio[1]. Pero no es hasta la novela "Neuromante" del autor de ciencia ficción William Gibson (1984), donde se cita por primera vez al ciberespacio, al referirse a todos los recursos de información y comunicación disponibles en las redes informáticas, especialmente en Internet.

Las TIC (Tecnología de la Información y el Conocimiento) en su aplicación al ciberespacio han revolucionado por completo la forma de relacionarse del hombre en una carrera meteórica que todavía es difícil ver el final. La globalización ha sacudido los pilares del Estado y las bases de nuestra sociedad, hasta el punto de que ha nacido una sociedad paralela a la física. Por esta razón, el ciberespacio se está convirtiendo en un punto de encuentro para millones de personas, gracias a su flexibilidad en el uso y a la cantidad de información que pone a disposición de los usuarios[2].

Esta nueva dimensión se ha convertido en un mundo colosal y complejo, donde las dimensiones espacio y tiempo no existen. En él se pueden encontrar, desde niños que casi no saben escribir, hasta profesionales de todas las ramas y niveles culturales. Pero, el problema está en que también está siendo usado por predicadores religiosos radicales, terroristas, ladrones y demás individuos con fines nada pacíficos.

Así, se puede constatar que no todo está siendo positivo en la irrupción del hombre en esta nueva dimensión. El gran peligro de la red reside en que, cuando se navega, no siempre se es consciente de los peligros y se tiene la sensación de hacerlo desde la más estricta intimidad y seguridad, que da la soledad. Pero en la red, a priori, está permitido un abanico grande de actividades que van desde lo decente a lo perverso. Mientras uno puede estar recreándose viendo un documental, leyendo un libro o haciendo una videoconferencia con un ser querido separado miles de kilómetros, otros pueden estar llevando a cabo acciones relacionadas con la pornografía infantil, robo, estafa, sabotaje, etc. Es por esta razón que los términos ciberdelincuencia, ciberterrorismo o ciberguerra son cada vez más conocidos, debido a que las noticias sobre acciones malvadas, relacionadas con el ciberespacio, son cada vez más frecuentes.

Ante el número creciente de informaciones que aparecen a diario sobre mal uso del ciberespacio, se tiene la sensación de que el ciberespacio se ha convertido es un "lugar" donde los actos pueden quedar impunes debido a sus dos características intrínsecas y principales: La ausencia de fronteras físicas y la dificultad de encontrar a los responsables y de que sean castigados. Además de estas razones, también habría que señalar que esta falta de regulación puede deberse a la novedad del fenómeno y los avances tan rápidos que se producen en él.

Ante este problema de posible vacío de normalización, que parece presentar el ciberespacio, el objetivo con el que se quiere afrontar este trabajo es estudiar en el momento actual los aspectos legales del mismo y como afectan a la ciberguerra. Para ello se plantearán una serie de interrogantes:

En la primera parte se tratará de dar respuesta a tres preguntas excluyentes, dado que sólo se pasará a la siguiente si las respuestas son afirmativas. La primera será sobre si existe un vacío legal en el ciberespacio. Caso de que se concluya con una afirmación, se pasará a debatir sobre si es o no necesario regularlo. Si se opta por la regulación, se analizará que opción es la mejor: Autorregulación o heterorregulación.

En la segunda parte, y dado que este trabajo se enmarca en un contexto de estrategia y seguridad, se analizará la ciberguerra y el Derecho Internacional Humanitario (DIH).

Junto a estos puntos principales se abordarán también los problemas éticos que suscita, las amenazas más importantes y la principal legislación (internacional y nacional) relativa al ciberespacio.

## Ética en el ciberespacio

La dependencia exponencial de nuestra sociedad del ciberespacio, hace que aumente la inquietud respecto del uso ético y legal que se puede hacer del mismo. Esta preocupación se hace mayor ante el dilema que plantea el aumento de posibilidades de comunicación y difusión de la información que nos ofrece la conexión a la red y los derechos fundamentales que se deben proteger.

El ciberespacio se está convirtiendo en un ejemplo claro de comprensión errónea del concepto de libertad. Algunos creen que la red de redes es el mayor espacio de libertad y que ésta disminuye conforme aumentan las restricciones, del mismo modo que harían dos magnitudes matemáticas inversamente proporcionales. Sin embargo, esta teoría es equivocada porque lo que ellos están defendiendo es el libertinaje y no la libertad. Locke dijo del libertinaje que "no se trata de una libertad sin límites sino del fin de la libertad porque se ha llevado a la libertad fuera de todo orden y se ha producido una negación de sí misma"[3].

La libertad en el ciberespacio, como en cualquier otra dimensión, debe entenderse con algunas limitaciones innatas (como puede ser la seguridad) porque si no fuera así estaríamos hablando de libertinaje. En este sentido, el catedrático de Filosofía F. Savater señala que "entre los valores que las instituciones deben de proteger y equilibrar, destacan la libertad y la seguridad"[4].

En primera instancia, ganar libertad en detrimento de la seguridad se podría considerar reaccionario y, sin embargo, ganar seguridad en detrimento de la libertad, podría ser catalogado como de dictatorial. El conflicto existe y es ahí hacia donde hay que dirigirse para tratar de resolver el problema, con la intención de encontrar un equilibrio.

Un ejemplo reciente de este conflicto, libertad versus seguridad, está en los descubrimientos que se hicieron entre 2012 y 2013, sobre el espionaje masivo que estaba llevando a cabo EEUU para justificar la lucha antiterrorista y que pusieron de manifiesto los planteamientos de lo que es ético o no. La defensa de estas acciones presenta retos importantes, por los valores que están en juego. F. Savater afirma que "cualquier política de cibervigilancia debería dotarse de normas claras (tanto legales como deontológicas) y tendría que estar acordada, al menos, entre los estados que comparten planteamientos democráticos semejantes"[5].

Como conclusión a este punto, un ejemplo claro de la necesidad de compaginar libertad y seguridad se puede constatar en el código de circulación. Cuando los primeros coches empezaron a circular por las carreteras no se vio la necesidad de un mínimo de normas que regularan el tráfico rodado. Hoy, con millones de vehículos en nuestras carreteras, unas normas de circulación y unos vigilantes son vitales para regular nuestro comportamiento al volante. En el ciberespacio ocurre lo mismo. La gran cantidad de ordenadores conectados a internet hacen necesario un "código de circulación, o mejor de actuación, para el ciberespacio".

## Principales amenazas en el ciberespacio

De las amenazas principales que tienen lugar en el ciberespacio señalaremos como más importantes el cibercrimen, el ciberterrorismo y la ciberguerra. Estas acciones están experimentando un fuerte apogeo que contrasta con la débil preparación de los Estados y organizaciones para hacerles frente.

### *Cibercrimen*

El cibercrimen comprende un amplio espectro de delitos entre los que cabría citar la piratería de software, juegos, música o películas; estafas, transacciones fraudulentas, acoso y explotación sexual, pornografía infantil, fraudes de telecomunicaciones, amenazas, injurias, calumnias, etc. Como se puede deducir, el cibercrimen persigue fundamentalmente conseguir un beneficio económico, pero también incluye el dominio de internet con fines inmorales.

Dentro del cibercrimen, la mayoría de los ataques informáticos provienen del uso del phising[6], troyanos[7] y los malware[8]. A través de los dos primeros, los delincuentes se pueden hacer con contraseñas que utilizan para obtener información sensible a la que habitualmente no tendrían permiso para acceder. Por su parte, los malware están evolucionando de forma alarmante en los últimos años. Su carta de presentación admite diferentes formas: virus, caballo de Troya, puerta trasera (backdoor), programa espía (spyware), o un gusano. Además, a causa de un malware pueden derivarse otros tipos de ataques como puede ser la denegación de servicio.

El cibercrimen se consolida como un negocio en alza. Los ataques informáticos podrían haber afectado a cerca de 378 millones de víctimas en todo el mundo, siendo los países más afectados: Rusia, China, Sudáfrica y Estados Unidos. Éste último lidera el coste, a escala mundial del cibercrimen[9].

***Ciberterrorismo***

El ciberterrorismo, aunque está muy vinculado con el cibercrimen, se diferencia de ésta en que no persigue principalmente un fin económico sino que se centra más en aquellas acciones en las que se persigue intimidar, coaccionar y causar daños con fines fundamentalmente políticos-religiosos.

El ciberespacio se está consolidando como un santuario de terroristas debido a que está siendo utilizado cada vez más por éstos. Las acciones que llevan a cabo en él pueden ser de financiación, guerra psicológica, reclutamiento, comunicación, adoctrinamiento, propaganda, entre otras.

Teniendo en cuenta que las guerras actuales se libran tanto en el campo de batalla como en la esfera de la información, la superioridad militar de un bando en el campo de batalla convencional, puede provocar que el más débil se focalice en la red con el fin de equilibrar la balanza de poder. Así, la invasión de Irak, comandada por Estados Unidos, brindó a la red un nuevo refugio, para los insurgentes, desde donde reorganizar su lucha contra las fuerzas occidentales de los “cruzados”[10].

La falta de regulación y el enmascaramiento que ofrece la red hace que los grupos terroristas realicen sus acciones con total impunidad. El cierre de sitios web no supone ningún problema para ellos ante la facilidad con la que encuentran nuevos servidores donde colocar sus páginas y seguir con sus actividades.

***Ciberguerra***

Hasta la aparición de Internet (1969) y su desarrollo (década de los 90), las guerras se habían llevado a cabo en los espacios terrestre, marítimo, aéreo y en el espacio electromagnético. Es a partir de la década de los 90 cuando la consolidación del crecimiento de la infraestructura tecnológica y el uso de las redes, hacen que cada vez se vea más al ciberespacio como un nuevo campo de batalla, donde se lleve a cabo la ciberguerra. Esta nueva forma de hacer la guerra no se limita solo a efectos sobre los equipos informáticos sino que sus consecuencias pueden trasladarse al mundo físico. Como defiende J.S Nye en su libro "El futuro del poder" (2010): "No se trata de una guerra sin derramamiento de sangre"[11].

Ante tal amenaza los Estados se están organizando. Si el dominio de las tres dimensiones tierra, aire y mar; supuso la creación de los Ejércitos de Tierra, Aire y Amada respectivamente. Hoy, los retos y amenazas que presenta el ciberespacio están haciendo que los Estados estén creando "ciberejercitos", que en el caso de España, se trata del Mando Conjunto de Ciberdefensa[12]. Sin embargo no creamos que todos están compuestos de personas uniformadas frente a un ordenador. La mayoría de los países están contratando a personal experto (muchos de ellos hackers conocidos) para que trabajen en estos cometidos. Las actuaciones de estos ciberejércitos ya se están haciendo notar.

Desde el punto de vista de la regulación de los conflictos, los gobernantes que recurran a la ciberguerra lo tendrán que hacer desde el respeto al ius ad bellum (el Derecho Internacional que rige la autorización del empleo de la fuerza por los Estados soberanos) y del ius in bello (el de la conducción de las hostilidades), mientras no se tenga ninguna regulación acorde a la regulación de estos nuevos conflictos (nueva o aclaratoria del DIH aplicado a la ciberguerra).

## Vacío legal versus regulación. Principal normativa

### *La necesidad y la dificultad de legislar*

Los juristas, al legislar, persiguen establecer las mínimas normas que rijan las relaciones, tratando de crear un marco que permita la convivencia y donde se respeten los derechos fundamentales.

Partiendo del hecho de que el acceso a las TIC y, por ende, al ciberespacio debe ser un derecho (El derecho al acceso a la red es contemplada por algunos países como el derecho fundamental. Así Finlandia reconoció en 2010 el derecho humano fundamental a Internet de banda ancha)[13], se debe proteger el libre uso del mismo en las condiciones anteriormente citadas de libertad y seguridad.

Para Roberto Gil Navalón, Jefe de la unidad SEGINFOPER, INS y DOC (Área de Seguridad de la Información (SDGTIC)), éstas serían algunas de las principales cuestiones relativas al ciberespacio que requieren de definición legal y que confirman el vacío legal de normativa aplicable a la red:[14]:

- Establecer hasta qué nivel el uso del ciberespacio es un derecho y cómo debe ser protegido.
- Determinar hasta dónde el Estado puede intervenir en nuestras acciones en el ciberespacio.
- Coordinar las acciones legales que, a consecuencia de actos en el ciberespacio, afecten a varias jurisdicciones.
- Congeniar en el ciberespacio el derecho a la intimidad con la necesaria identificación de los delincuentes y la obtención de la evidencia del delito.
- Determinar qué nuevos delitos pueden existir que sean exclusivos de acciones en el ciberespacio.
- Acordar las limitaciones al posible uso del ciberespacio en los conflictos bélicos.

Esta necesidad de regular estos aspectos citados son una prueba más de que el vacío legal, en nuestras relaciones en el ciberespacio, es notorio. La sensación de desamparo crece ante las amenazas que se ciernen en el creciente uso de la red en nuestras actividades cotidianas. El ciberespacio, como realidad virtual en la que cada vez más interactuamos, debe estar regido por unas mínimas normas, al igual que cualquier otro ámbito de nuestra actividad diaria social (el tráfico vial, la compra y venta de un inmueble, etc.). Sin embargo, las relaciones en el ciberespacio no son más que datos, secuencias de bits, que viajan de un lado a otro y de los que será difícil determinar la verdadera finalidad de los mismos. Desde el punto de vista técnico, no hay diferencia aparente entre la secuencia de datos de un simple correo personal particular y de un ciberataque (paralizar el sistema bancario), cibercrimen (robo) o ciberterrorismo (ataque de sabotaje en una central eléctrica).

La regulación no será fácil debido a las características de esta realidad virtual. A la ya citada ausencia de fronteras (que acerca a las personas pero también a los delincuentes) y a la dificultad de identificar a los que están ciberactuando con intenciones maliciosas, habría que sumar la rápida difusión de las acciones (pero no necesariamente de los efectos), son prueba de la dificultad de su normalización.

El gran problema que se les presenta a los que defienden una regulación es la lentitud intrínseca de las regulaciones nacionales e internacionales ante los rápidos avances tecnológicos, debido a la falta de preparación ante estos nuevos retos. Ésta es una de las razones por la que la red es tachada de pesadilla jurídica.

Mientras tanto la intranquilidad se va haciendo patente cuando leemos frases como "Internet era una esperanza; nos la han robado" e "Internet es un sueño para los usuarios y una pesadilla para los prácticos del Derecho"[15].

### *Regulación versus libertad absoluta*

Visto en el punto anterior el vacío legal y la sensación de indefensión, sería conveniente analizar si son necesarios regular los modos de comportamiento en

el ciberespacio o si, por el contrario, se debe de entender como un "lugar" de libertad absoluta.

Algunos expertos mantienen que el ciberespacio es enormemente regulable y estiman necesario que dicha regulación se haga a través del Derecho. Si con unas normas de cortesía no basta para que la sociedad funcionara correctamente[16], menos lo sería en las relaciones que establezcan sus miembros en el ciberespacio, debido a la gran cantidad de delitos que se cometen y la dificultad de encontrar a los autores para que respondan de sus hechos.

El Derecho debe irrumpir en el ciberespacio como, por ejemplo, lo hizo con el espacio aéreo y las aguas territoriales. Su objetivo es demostrar que ese espacio de libertad absoluta, que algunos consideran, es una utopía. El ciberespacio es una prueba más que confirma que el ser humano no puede vivir en un mundo ni sin normas y ni con sólo normas de cortesía. Las normas jurídicas son necesarias porque la ausencia de las mismas ha conducido al descontrol y al libertinaje.

Por tanto, se requiere de un cuerpo normativo, ad hoc, que regule los comportamientos en el mismo. En la redacción del mismo deben participar expertos en las TIC y en Derecho debido a que la tecnología y sus avances pueden dificultar su regulación.

En definitiva se tratará de que muchos de los delitos que han llegado al ciberespacio, procedentes del mundo físico, puedan quedar impunes y si son juzgados se haga desde el máximo respeto a las Leyes.

En el extremo opuesto a la Regulación están los que defienden la Libertad Absoluta. J. Perry Barlow así lo hizo en la Declaración de Independencia del Ciberespacio[17]:

"Gobiernos del Mundo Industrial (…). No son bienvenidos entre nosotros. No tienen ninguna supremacía donde nos juntamos…El Ciberespacio está fuera de sus fronteras…Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o al inconformismo. Sus partidarios no consideran que ningún Estado ni Organización deba participar en la regulación, al considerar que el ciberespacio es un espacio de libertad".

Queda claro, tras leer algunos fragmentos, que esta Declaración está llena de afirmaciones populistas ya que es difícil concebir un lugar sin regulación.

Para los partidarios de esta "utopía", cualquier intento de regulación podría catalogarse como de censura. No creen que la libertad de expresión, de acceso a la información, etc; deban ser sometidos a condiciones. Por otro lado, tampoco creen que la complejidad tecnológica que da soporte al ciberespacio, pueda admitir una ordenación efectiva y completa.

La primera de las razones anteriormente expuestas, en contra de la regulación, roza la fantasía (el ciberespacio como lugar de libertad plena), si tenemos en cuenta que cada día conocemos múltiples noticias sobre acciones ilegales en la red.

Por otro lado, si podría ser cierto que la regulación de una red virtual y tecnológica entrañará sus dificultades. Sin embargo, el Derecho no pueden mirar hacia otro lado ante los atropellos, que se conocen (y otros que no), y que se suceden en el ciberespacio.

Se ha demostrado que el hombre no quiere vivir solo y que, dado que quiere vivir en sociedad, las normas de cortesía o morales no son suficientes. A pesar de que la Ley no puede abarcarlo todo, como afirmaron San Agustín y Santo Tomás de Aquino[18], si deberá de hacerlo, como sucede en el ciberespacio, cuando se pueden ver gravemente afectadas la libertad y la seguridad de los individuos.

Una vez analizado los pros y los contras, parece claro que el comportamiento en la red, sin un mínimo de "control", no tiene cabida en ningún Estado y menos en las sociedades democráticas. No debe haber espacio que pueda hacer sospechar que la libertad y la seguridad de los cibernautas, no están protegidos. En el caso de optar por no legislar, el libertinaje sería quien gobernaría la red liderada por unos pocos. El resto tendría que aguantar los atropellos y las injusticias de los ciberdelincuentes.

***Autorregulación versus heterorregulación.***

Una vez afirmada la necesidad de regulación del ciberespacio, queda plantear la tercera pregunta de la primera parte de este trabajo: ¿La regulación del ciberespacio se hará desde la autorregulación o desde la heterorregulación?

La autorregulación hace referencia a una regulación desde el interior de la red por los usuarios de la misma. Se basa en la confianza mutua y la responsabilidad compartida de los usuarios. Por tanto, aquí se produce un desplazamiento en el ajuste normativo desde los juristas hacia los usuarios y empresas relacionadas con el sector de las TIC, para operar en el ciberespacio.

Los defensores de la autorregulación lo hacen, principalmente, en base a los problemas que pueden surgir, ante cualquier actividad que sobrepase las fronteras físicas: la internacionalidad de la red y la dificultad para imponer reglas a los participantes. M. Asensio señala que "el ciberespacio constituye en cierto sentido una zona independiente transnacional y ajena a jurisdicciones y territorios estatales"[19].

Algunas de las ventajas que presentaría la autorregulación serían:

- Si internet surgió como el espacio de máxima libertad, y puesto que hay que elegir entre autorregulación o heterorregulación, parece claro que es la primera, la única opción factible en el camino de la normalización.
- La autorregulación, por los propios actores, podría ser la elección más adecuada para el arbitraje.
- A través de la autorregulación sería más fácil y rápido crear un sistema normativo internacional que no dependiera de fronteras físicas. Así sería válido en todas las partes del mundo, amparado por la globalización.
- Se trata del remedio que mejor se adapta a los cambios tecnológicos.

Sin embargo, las desventajas que presenta la autorregulación son:

- La ordenación sería llevada a cabo en base a normas éticas.
- La exigencia de responsabilidades no es tarea fácil porque en los entornos electrónicos estos actores no son siempre identificables o pueden encontrarse fuera de alcance.
- La autorregulación hace que la responsabilidad de impartir justicia y aplicar sanciones recaiga en los propios usuarios de la red.
- La autorregulación carecería de la más mínima legitimidad democrática que tienen que poseer las normas que van a tener un alcance global. La soberanía nacional que defiende nuestras constituciones no tiene cabida en la autorregulación.
- La autorregulación podría dejar sin protección derechos que los Estados defienden y que de ninguna manera deben de renunciar, a pesar de las características de esta dimensión.

Ni los que más apuestan por esta forma de regular lo hacen desde convicciones absolutas. Así E. Suñé Llinás señala en la "Declaración de Derechos del Ciberespacio": Conscientes asimismo de que la libertad, como decía su apóstol John Locke, pasa por la intervención mínima del poder, lo que supone la necesidad de dejar amplios espacios abiertos a la autorregulación; pero siempre dentro de un marco legal que sea de veras orden de libertad[20].

Como se puede ver, las desventajas superan a las ventajas, en el caso de la autorregulación. Ésta se puede prestar al subjetivismo de inexpertos del mundo jurídico y a que, en el caso de aplicar justicia, se estaría cerca de "tomarse la justicia por su mano". Además, un Derecho creado por los internautas es incompatible con la idea de soberanía nacional y democracia.

Por las carencias presentadas anteriormente, se considera que la mejor forma de regular el ciberespacio es la heterorregulación, en contraposición a la autorregulación. La heterorregulación hace referencia a una regulación desde fuera de los usuarios, ya sea por el legislador nacional, bien por acuerdos internacionales, por parte de acuerdos entre Estados y Organizaciones Supranacionales. Los gobiernos tienen la obligación de proteger los derechos fundamentales de sus ciudadanos en cualquier dimensión en la que actúen (tierra, mar, aire y por qué no en el ciberespacio).

Los motivos, que hacen de la heterorregulación la mejor herramienta, se deben a las siguientes razones:

- Si una sociedad autorregulada no es posible, porque sería una utopía, tampoco lo puede ser el ciberespacio. Así no se ve otra solución que pensar que el Derecho, a través de las instituciones, deberá entrar en esta cibersociaedad. La sociedad se ha mostrado incapaz de respetar deontológicamente una normativa, por lo que se estima necesaria la intervención de alguna instancia ajena a la sociedad de Internet, alguien que vele por el orden y por el respeto de los derechos y libertades[21].

- La heterorregulación no es más que la consecuencia de la defensa de los Derechos Fundamentales de los ciudadanos contemplados en las constituciones democráticas.

- El ciberespacio ofrece un medio fácil y rápido de llevar a cabo actividades, sin desplazarnos y que nos permitan ahorrar tiempo (pensemos que ya no necesitamos ir al banco para hacer una transferencia). Si estos trámites están regulados (cuando nos presentamos en el banco con nuestro DNI,...) por qué no lo iban a estar si se realizan a través de internet.

A pesar de que las ventajas de la heterorregulación superan a las de la autorregulación, se es consciente de las dificultades de hacerlo. A los problemas ya citados se sumarán que en el ciberespacio conviven diferentes tipos de redes, usuarios de diferentes costumbres, éticas y moralidad. Es por esto que los acuerdos de mínimos en normas se deben alcanzar desde el consenso internacional.

Entre tanto, la autorregulación podría ser:

- Una solución a corto plazo en el camino de su regulación. Podría ser aceptada como un paso intermedio, en caso de ausencia (por inexistencia o porque se está regulando en ese momento) de legislación procedente de la heterorregulación. Esta forma de regular se debe hacer por parte de juristas pero contando con la opinión de los expertos en el campo de las nuevas tecnologías.

- Una forma de compartir la regulación con la heterorregulación. Aspectos como caducidad de password, páginas WEB, comportamientos no éticos (contenidos inapropiados en páginas según edades, etc); podrían ser objeto de la autorregulación y otras más transcendentales como los ciberdelitos, ciberguerra, etc; se podrían regular desde la heterorregulación.

## *Principal normativa internacional y nacional*

Una vez planteado la cuestión sobre el vacío legal en el ciberespacio y las posibles formas de regularlo, se van a exponer la principal normativa que existe tanto en el plano internacional como nacional. Ésta no es sólo escasa sino que tampoco hay voluntad, por parte de los Estados, para su cumplimiento.
La OTAN, durante la conferencia de Praga de 2002, decidió poner en marcha un programa global de coordinación de la ciberdefensa, con el objetivo de reforzar las capacidades de la Alianza y luchar contra los ataques informáticos. No fue hasta después de los acontecimientos de Estonia (2007), cuando se decidió a trabajar con el objetivo de definir un nuevo concepto estratégico de política de ciberdefensa, el cual fue el resultado de la Cumbre de Lisboa (2010). Así, y como resultado de esta Cumbre, los ministros de defensa de la OTAN aprobaron el 8 de junio la nueva política de ciberdefensa. En él se contemplan los ciberataques como acciones que pueden poner en riesgo la prosperidad, la seguridad y la estabilidad de los Estados miembros y se marcan directrices y recomendaciones en el área de la ciberdefensa. En general, la OTAN ha tomado el criterio de que son los países miembros los que tienen que proteger sus redes en base a medios (software y hardware) y a una regulación desarrollada, teniendo en cuenta lo aprobado en la citada Cumbre.

En cuanto a Naciones Unidas, aunque la regulación del ciberespacio, a priori, pudiera parecer enfrentarse a los mismos problemas a los que se tuvo que enfrentar la regulación de las aguas territoriales o a la del espacio aéreo, el resultado final no ha sido el mismo. En el caso del "alta mar" (nombre jurídico de las aguas internacionales) siempre había imperado una costumbre internacional de libre navegación y que se plasmó en un tratado internacional en 1958 y sus posteriores reformas hasta la III convención del Derecho del mar en 1982.

Hasta el momento, las iniciativas para la regulación del ciberespacio, por parte de las NNUU, han sido escasas y sólo afectan a aspectos concretos. No se ha logrado, hasta el momento, un consenso internacional debido fundamentalmente a que por su novedad material, no existen normas consuetudinarias al respecto (como se ha señalado que si existían en el caso de las aguas internacionales). En este sentido es de destacar la falta de consenso en el año 2010 para aprobar una propuesta de tratado entre los estados contra el cibercrimen. A pesar de las discrepancias surgidas, se establecieron acuerdos globales, en base a unas reglas de mínimos, con principios básicos y esenciales para ser tenidos en cuenta en el desarrollo de las normas nacionales.

Por parte de NNUU las principales resoluciones en esta área son:

- Resoluciones de la Asamblea General 55/63 (2000) y 56/121 (2001). A través de estas resoluciones se **invita** a los Estados Miembros a que tomen en cuenta las medidas propuestas, al elaborar leyes y políticas nacionales, para combatir la utilización de la tecnología de la información con fines delictivos.
- Resoluciones de la Asamblea General 57/239 (2002) para la creación de una cultura global de ciberseguridad. A través de esta resolución

se **exhorta** a crear la citada cultura teniendo en cuenta los principios de: conciencia, responsabilidad, respuesta ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación.

- Resolución de la Asamblea General 58/199 (2004) para la protección de las infraestructuras de información. Se persigue **estimular** el desarrollo de normas de conducta en el ciberespacio que sirvan para la promoción del desarrollo socioeconómico y el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información.

Como se puede constatar de los fines de estas resoluciones (invitar, exhortar, estimular, etc.), éstos se limitaron a dar, en su mayoría, recomendaciones y observaciones, que pudieran ser un punto de partida para las regulaciones nacionales.

Pasando al Consejo de Europa, como organización destinada a promover la cooperación entre los Estados Europeos, ésta ha sido la primera organización internacional en adoptar un tratado para la lucha contra los delitos en internet. El Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest) entró en vigor el 1 de julio de 2004 y fue ratificado por 35 Estados miembros (la mayoría perteneciente a la UE) y por otros como los Estados Unidos.

Se trata del primer tratado internacional en hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Incluye aspectos legales como la jurisdicción y la extradición; también establece medidas de coordinación como la asistencia mutua para establecer un contacto permanente entre todas las autoridades competentes de los Estados firmantes.

En definitiva trata de aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. Se podría tratar de una referencia como legislación global en el ciberespacio. El objetivo ahora es que los países traten de desarrollar su normativa nacional en base a este convenio, en materia de seguridad informática.

Pasando ahora al caso de la Unión Europea, en mayo de 2010, la Comisión Europea presentó una comunicación titulada *Una Agenda Digital para Europa*. Esta constituye uno de los siete pilares de la Estrategia Europa 2020, para fijar objetivos que permitan el crecimiento de la Unión Europea hasta el 2020. El fin que persigue es proponer explotar mejor el potencial de las tecnologías de la información y la comunicación (TIC) para favorecer la innovación, el crecimiento económico y el progreso. Entre las acciones que presenta destacan

la propuesta de establecer normas en materia de jurisdicción en el ciberespacio a nivel europeo e internacional y la de medidas para combatir los ciberataques.

La UE en la Decisión marco del Consejo de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, señala una serie de delitos que darán lugar a la entrega, en virtud de una orden de detención europea, siempre que estén castigados en el Estado miembro emisor con una pena o una medida de seguridad privativas de libertad de un máximo de al menos tres años. Entre esta serie se encuentran "los delitos de alta tecnología, en particular delito informático"[22]

Y, por último, unas palabras sobre la legislación española. La jurisdicción nacional, y siguiendo la tendencia de los países de nuestro entorno, ha hecho pocos avances en este campo. Por lo tanto, trata de aplicar las leyes vigentes aplicándolas para el caso del ciberespacio. Así, el Código Penal se aplica a delitos en el ciberespacio que se interpretan contemplados en el Capítulo II (De las amenazas) del Título VI (Delitos contra la libertad), Capítulo V (De los delitos relativos a la prostitución y la corrupción de menores) del Título VI (Delitos contra la libertad e indemnidad sexuales), Capítulo I (Del descubrimiento y revelación de secreto) del Título X (Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio), Capítulo II (Injurias) del Título XI (Delitos contra el honor), entre otros.

Como ejemplo reciente de detenciones por injurias en redes sociales, tenemos las últimas acciones llevadas a cabo por la policía contra los comentarios aparecidos en Twitter, con ocasión del asesinato de la Presidenta de la Diputación de León (12 de mayo de 2014). Sin embargo, no es hasta el año 2010 cuando se introducen en el Código Penal dos nuevos delitos con aplicación casi exclusiva al ciberespacio. El primero es relativo a las alteraciones en sistemas informáticos ajenos o la interrupción de su funcionamiento. El segundo afecta al acceso a los sistemas sin autorización, vulnerando sus medidas de seguridad. También es novedoso que esta ley introdujese la posibilidad de responsabilidad penal de las personas jurídicas por ataques a sistemas informáticos.

Del mismo modo, en la legislación española se han desarrollado varias leyes sectoriales que tratan explícitamente el asunto exclusivo del ciberespacio: La Ley Orgánica de Protección de Datos 15/1999, la Ley General de las Telecomunicaciones 32/2003 y la Ley de Servicios de la sociedad de la información y de comercio electrónico 44/2002, entre otras.

## La ciberguerra y el Derecho Internacional Humanitario

### *Manual de Tallín*

En abril de 2007, y en represalia por el traslado en Tallin del monumento a los soldados soviéticos caídos durante la Segunda Guerra Mundial desde el centro de la ciudad hasta el cementerio militar, se produjeron unos ciberataques contra los sistemas de información del gobierno estonio, por agresores no

identificados. El resultado fue la paralización de gran parte de la administración de Estonia.

Estos ciberataques marcaron un antes y un después en lo relativo a la ciberguerra. La consecuencia más inmediata fue que la OTAN decidió establecer en su capital, Tallín, el Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (CCD COE). Su misión es la congregar los esfuerzos de sus Estados miembros (Estonia, Letonia, Lituania, Alemania, Hungría, Italia, Polonia, Eslovenia, España, Holanda y Estados Unidos) para mejorar la capacidad de intercambio, cooperación e información entre la OTAN, sus Estados miembros y terceros estados socios de la OTAN; en asuntos relativos a la defensa cibernética en virtud de la educación, la investigación y desarrollo, las lecciones aprendidas y las consultas[23].

Como consecuencia de la falta de legislación aplicable a las nuevas guerras en el ciberespacio, una de las primeras iniciativas de este Centro, fue la convocatoria de un Grupo Internacional de Expertos (GIE) en defensa, ciberseguridad y Derecho internacional, para que trabajaran en lo que pudiera ser el equivalente de la Convención de Ginebra sobre el DIH, aplicado a los conflictos en el ciberespacio. El resultado fue el Manual de Tallín, que fue dirigido por el Profesor Michael Schmitt de la US Naval War College, y que se presentó en Londres el 15 de marzo de 2013.

La premisa fundamental con la que se empezó a redactar este Manual fue que la guerra no deja de ser tal porque se lleve a cabo en el ciberespacio, es decir, es posible la guerra en el ciberespacio. Aunque a fecha de hoy no se tengan datos empíricos reales sobre los efectos de las ciberarmas, sólo algunos hechos como los de Estonia (2007) y Stuxnet (2010), se cree que no es ciencia ficción y que sus posibilidades pueden ir más allá de una denegación de servicio. Antes de que sea demasiado tarde, es necesario poner de relieve que ciertas acciones, como por ejemplo, penetrar ilegalmente en los ordenadores centrales de control de una presa y conseguir descargar el agua, pueden tener el mismo efecto que si se volaran con explosivos las compuertas y el agua pudiera salir de la misma.

En definitiva, los objetivos que se querían alcanzar con este Manual, eran los siguientes[24]:

- Interpretar, por primera vez, las normas existentes a los ciberataques.
- Unir el mundo ciber con el jurídico en sus análisis y sus comprensiones mutuas.
- Valorar la capacidad de los Estados de buscar el consenso sobre los límites éticos y jurídicos en el ciberespacio, especialmente en lo que respecta a la agresión armada y el empleo de la fuerza.
- La falta de anticipación a las incertidumbres actuales sobre las normas aplicables al ciberespacio podría tener, en el futuro, consecuencias desastrosas. Así lo señala el Profesor Jack Goldsmith (Harvard): "Un Estado podría emprender una operación cibernética que otro clasificara

como acto de guerra, incluso cuando la primera nación no tuviera la intención de emprender semejante acción"[25].

Este Manual **intenta ser** una herramienta para los juristas que quieran tener una visión global de los desafíos jurídicos internacionales relacionados con la conflictividad en el ciberespacio. Si el mar, el aire y la tierra son ya campos de intervención reglamentados, por qué razón no lo iba a ser el ciberespacio.

Un valor añadido de este Manual es que cada norma definida tiene asociada una explicación que describe cómo el GIE interpretaría las normas aplicables en el contexto cibernético. También recoge los desacuerdos del grupo en cuanto a la aplicación de las mismas, caso de que los hubiera habido. Conviene aclarar, no obstante, que no se trata de un documento oficial que refleje la doctrina oficial de la OTAN, ni la postura de las organizaciones o estados representados, ni tampoco la del propio centro, sino que sólo recoge las opiniones de un GIE independientes.

En cuanto a sus contenidos y estructuras, éste Manual se compone de 95 reglas dispuestas en dos partes (La seguridad del ciberespacio en el Derecho Internacional y El Derecho Internacional de los conflictos cibernéticos) y siete capítulos. Algunas de estas reglas son una copia casi idéntica de los artículos de convenios ya existentes y otras una adaptación al caso de acciones en el ciberespacio. Todas ellas reflejan el consenso existente en esta materia y van acompañadas de comentarios que incluyen las fuentes utilizadas y aportan un análisis detallado de la lógica seguida en su redacción.

En definitiva, estas interpretaciones sobre la ciberguerra desde el punto de vista del DIH son incompletas ya que hubo falta de consenso en aspectos fundamentales. A continuación se van a analizar algunas de las cuestiones más controvertidas.

### *Aspectos claves del Manual*

A continuación se va a estudiar la ciberguerra y el DIH. Como se va a poder observar, hay algunos aspectos de esta forma de conflicto que pueden crear innumerables controversias, al querer tratar de regularlo, desde este prisma. Las particularidades, la forma de actuar y los actores que tienen cabida en el ciberespacio, entre otros; provocarán innumerables comentarios y discrepancias sobre esta forma de poder llevar a cabo la guerra.

### a) Ciberataque y conflictos del DIH.

Partiendo de la definición de ciberataque como aquella operación cibernética ofensiva o defensiva de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas y daños o destrucciones de bienes[26]; se puede ver que este tipo de acción entra dentro de la definición contemplada en el artíc. 49 del Protocolo Adicional I a los Convenios de Ginebra.

El primer aspecto controvertido es determinar si cualquier operación de ciberguerra puede ser considerada como "un conflicto armado" y, por tanto, puede regularse a través del DIH. En este sentido, surgen dos puntos de vista: los que afirman que cualquier ciberataque tendría cabida y los que piensan que debería existir una relación directa entre la operación y los objetivos militares. Parece lógico pensar que no todas las acciones que se lleven a cabo podrían tener cabida. La razón es que durante el conflicto, se pueden producir infinidad de ciberataques por actores estatales y no estatales, a priori, de difícil descubrimiento y, caso de hacerlo, de complejidad en definición.

Algunos miembros del GIE señalaron que las acciones de ciberguerra entre Rusia y Georgia (2008) si lo fueron debido a que se efectuaron en el seno de un conflicto armado. Sin embargo, los "supuestos" ciberataques de Rusia contra Estonia (2007) no porque no fueron parte de un conflicto. Además, el gran número de ciberataques y lugares diferentes desde donde se llevaron a cabo dificultó la asignación de responsabilidades. A pesar de que se sospecha que Rusia estaba detrás de ellos, en ningún momento se ha podido demostrar que su culpabilidad.

**b) Soberanía y responsabilidad.**

La soberanía de un Estado también puede ser violada por ataques desde el ciberespacio. Los Estados deberán controlar las infraestructuras cibernéticas[27] que se encuentren en su territorio o que actúan bajo su bandera, sin estar en sus límites geográficos.

La duda aquí surge sobre la responsabilidad del Estado ante acciones cibernéticas que se lleven a cabo desde su territorio o que transiten por él, sin que se pueda comprobar que tuviera conocimiento ni capacidad para detectarlas. Parece lógico pensar que sólo en el caso de tener conocimiento de ello y no haber puesto los medios o informarlo, en caso de no tenerlos, podría incumplir la ley.

Otro aspecto que crea problemas es el control de un Estado por las acciones que se puedan llevar en su nombre. Así, se considerará ***"hecho del Estado***", según el derecho internacional, "*el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento*"[28]. Los ciberataques que sufrió Estonia (2007) si fueron un atentado a su soberanía sin embargo, y a pesar de las evidencias, no se pudo culpar a Rusia porque en ningún momento se pudo comprobar el más mínimo control sobre el caos originado. No existe prueba alguna de que el grupo de hackers operara bajo control de ningún Estado.

Otro caso anterior, aunque no tuvo como protagonista los ciberataques, fue el apoyo que prestó EEUU a la Contra de Nicaragua. En este caso no se responsabilizó a EEUU por hechos internacionalmente ilícitos porque, a pesar de probarse que estaba financiando a este movimiento, no se pudo comprobar

que dirigiera sus acciones (control efectivo o total). Como se puede comprobar el aspecto del "control" es bastante ambiguo y está también presente en el ciberespacio.

Ni que decir tiene que acciones en las que un Estado presta ayuda o asistencia a otro Estado y/o lo dirige en la comisión por este último de un hecho internacionalmente ilícito, también puede tener que responder por hechos internacionalmente ilícitos[29].

En respuesta a las mismas, cualquier Estado podría recurrir a mecanismos de respuesta (contramedidas) con el objeto de que el Estado agresor se reanude en el cumplimiento de sus obligaciones[30], cesando en su comportamiento ilegítimo. Sin embargo estas contramedidas no podrán afectar, de ninguna de las maneras a las obligaciones de carácter humanitario que prohíben las represalias ni incumplir el principio de proporcionalidad[31]. También se excluyen de estas contramedidas las relativas al uso de la fuerza[32]. Sin embargo, dentro de la Resolución de la Asamblea General 56/83 de las NNUU, también se dice que los artículos se entenderán sin perjuicio de lo que exprese la Carta de las NNUU[33], y esta expresa en su artic. 51 el derecho inmanente a la legítima defensa…en caso de ataque armado (posteriormente se analizarán los ataque armados y el ciberespacio).

**c) Uso de la fuerza.**

Si los criterios que aparecen en la Carta ofrecen múltiples interpretaciones para determinar cuándo un acto constituye un "uso de la fuerza" (artíc. 2.4), el ciberespacio no hace más que aumentar el problema y crear más ambigüedad.

Para tratar de solucionar la cuestión se tendrá en cuenta los aspectos que más íntimamente están ligados con el "uso de la fuerza": la escala (grado/umbral) y los efectos. En el caso de un ciberataque, a priori, serán determinantes los efectos, los cuales deben ser comparables a los de un ataque convencional.

A continuación se citan una serie de indicios que van a ayudar a determinar si una acción en el ciberespacio, es un "uso de la fuerza" o no[34]:

- **Gravedad:** Se trata del factor más importante y la cuestión fundamental será determinar cuáles son los límites que, una vez sobrepasados, determinan que se ha hecho "uso de la fuerza". El alcance, la duración y las consecuencias tendrán gran importancia en la valoración de su gravedad de la acción. En resumen, se tratará de responder a cuestiones como: ¿cuántas personas han muerto?, ¿qué daños se han causado?, etc.

- **Inmediatez:** Tiene que ver con la separación temporal entre acciones y efectos. Muchas acciones en el ciberespacio no producen efectos inmediatos sino que éstos aparecen con el paso del tiempo. Cuanto mayor sea la separación acción-efecto, más complicado será la posibilidad de afirmar que se ha hecho "uso de la fuerza".

- **Intrusión:** Se refiere al grado de penetración o alcance de las operaciones. Así, por ejemplo, no todos los dominios en el ciberespacio tienen la misma importancia (no es lo mismo uno que acabe en "...@.mdef.es", del Ministerio de Defensa de España que uno particular, tipo "...@gmail.com") y, por tanto, el grado de intrusión no es igual en ambos casos.

El ciberespionaje, que podría ser otra forma intrusión, no está considerado como un "uso de la fuerza". Un ejemplo serían las acciones para deshabilitar los mecanismos de seguridad y acceder a la información de una red. Sin embargo, un avión que penetra en un espacio aéreo, sin autorización y con intención de llevar a cabo acciones de ciberespionaje, si podría ser acusado de"uso de la fuerza".

- Carácter militar e implicación del Estado: Cuanto mayor sea la relación o nexo entre las ciberoperaciones y las operaciones militares, mayor será la probabilidad de ser considerado un cibertaque como de "uso de la fuerza".

- La presunción de legalidad: El DIH es por naturaleza prohibitivo. si algo no está prohibido estaría autorizado. El ciberespionaje, no parece que suponga una violación del DIH, en cuanto a ser considerado como "uso de la fuerza". A priori, no supone ni una violación del principio de no intervención ni siquiera un elemento coercitivo, aunque para ello tenga que superar elementos de seguridad (cortafuegos,...). Acciones de denegación de servicio, como los llevados a cabo en el caso de Estonia y que paralizaron su administración, no se consideraron tampoco como una violación del "uso de la fuerza".

### d) Ataque armado

La determinación de "ataque armado", íntimamente ligado al de "uso de la fuerza", también presenta discrepancias en el caso del ciberespacio. Se trataría ahora de determinar que "artefactos", al ser usados, pueden dar lugar a un ataque armado. Sin embargo, y en la misma línea del punto anterior, parece que lo verdaderamente importante son las consecuencias que se deriven de su uso, y si estas, podían ser equiparables, por su gravedad a un ataque armado, y por ende, a un uso de la fuerza.

Se podrían considerar como "ataque armado", aquellos ciberataques que hieren, matan o destruyen propiedad y no lo serán aquellos que guardan relación con inteligencia, robo y en general aquellos que no interrumpen servicios esenciales (un hipotético ataque a una central distribuidora de agua para envenenamiento y que provocara enfermedades, no hay duda de que sería un ataque armado). Sin embargo, a día de hoy, no se ha considerado ningún ciberataque como ataque armado. De las dos principales acciones, Stuxnet y Estonia, sólo la primera parece haber alcanzado el umbral de la consideración de ataque armado, debido a que supuso la paralización total del programa nuclear. Además, todo apunta a que sea el primer uso, por parte de una nación, de un

programa malicioso como arma informática contra la infraestructura de otra nación. Además, este incidente resulta significativo porque, hasta la fecha, inhabilitar una instalación de este tipo sólo habría sido posible mediante alguna acción física, por ejemplo un bombardeo[35].

**e) Legítima defensa. Inminencia e inmediatez**

Si en el ciberespacio se ha determinado que se pueden dar casos de "uso de la fuerza", también tendrá cabida la "legítima defensa", en respuesta a los mismos. Esta afirmación se justifica con más argumentos si el "uso de la fuerza" es con ocasión de un ciberataque considerado como "ataque armado". En este sentido, el artíc. 51 de la Carta de las NNUU reconoce el derecho a la legítima defensa.

Dentro de este apartado, es necesario comentar que también en el ciberespacio, como ocurriría en el caso de armas nucleares, se puede aprobar la "legítima defensa anticipada" (inminencia). Aunque este tema ha planteado muchos debates, parece que ésta sólo se pudiera aprobar en el caso de que, de no llevarse a cabo y el Estado esperara a sufrir un ciberataque, éste hubiera perdido cualquier oportunidad de responder ante los efectos del mismo (la relación causa-efecto debe estar muy justificada).

Relacionado con la "legítima defensa" también estaría el principio de inmediatez. El requisito de "inmediatez" (a diferencia de la exigencia de la inminencia) distingue un acto de legítima defensa de la mera represalia. Si la "inminencia" plantea discusiones, la "inmediatez" lo es más ante el tiempo que puede transcurrir hasta que se descubran los efectos y la identificación de los culpables. Esto se debe a que los efectos de los ciberataques no siempre serán conocidos de inmediato y por lo tanto no será fácil verificar si se ha recurrido al "uso de la fuerza" que determine una respuesta del tipo "legítima defensa".

De cualquiera de las maneras la legítima defensa estará siempre limitada por los principios de necesidad, proporcionalidad y distinción; según las normas del DIH.

**f) Principio de necesidad y proporcionalidad.**

La ciberguerra puede ser un medio recurrente para los actores que se enfrentan a oponentes con los que existe una gran desequilibrio en recursos militares (personal, material, tecnología, etc). Esta asimetría de medios, también puede completarse con una asimetría de valores provocando que la ciberguerra sea parte de una "guerra sin restricciones".

Estas acciones deben responder al principio de necesidad de tal forma que se consiga un equilibrio entre las necesidades de la guerra y los condicionamientos humanitarios. En definitiva, se aplicaran ciberataques de tal grado que sus efectos sean los mínimos necesarios para conseguir el objetivo deseado, que es hacer que el enemigo cese en sus acciones.

La proporcionalidad hace referencia a la prohibición de armas y métodos que causen en las personas civiles y a sus bienes, o a ambos a la vez, daños excesivos con respecto a la ventaja militar concreta y directa prevista. Tras esta afirmación se plantea dos cuestiones:

- Si hay alguna limitación o prohibición en cuanto a las ciberarmas. Todo parece apuntar que los efectos serán el factor que las delimite. Así pues, el alcance, duración e intensidad será el mínimo que haga al agresor desistir de sus acciones. No obstante, si la respuesta en forma de ciberataques, no fueran suficientes para detener la aptitud violenta del agresor (porque técnicamente no le afectan debido a que dispone de contramedidas que les hace inmunes), se podría hacer uso de acciones cinéticas.

- El término "excesivo" no ha sido cuantificado. A pesar del comentario contradictorio del CICR, los expertos consideran que solo se autorizan los daños colaterales cuando la anticipación concreta y directa de la ventaja militar es suficiente respecto al ataque en su conjunto[36].

**g) Participación directa en las hostilidades.**

La participación directa en las hostilidades es otra cuestión que genera numerosas controversias en las nuevas formas de actuación en los conflictos (Artículos 51.3 del Protocolo adicional I y 13.3 del Protocolo adicional II).

Los civiles (a veces de forma individual tipo "lobo solitario") podrían llevar a cabo ciberataques que tengan relación directa con las hostilidades, con los efectos ocasionados y a favor de una de las partes, por simpatizar con ellas.

El problema de estas acciones es la variable "tiempo". Los expertos, mayoritariamente, consideran que la participación comprende desde el momento de la preparación de la misión hasta el final de la participación activa. Así, Rodríguez-Villasante afirma que "el carácter directo de la intervención se extiende a la preparación o al retorno desde el lugar atacado[37]. Relacionado con esto, durante los conflictos de Irak y Afganistán se ha puesto de moda el concepto de "puerta giratoria" o "revolving door", es decir, aquellos individuos que en un momento determinado deciden participar de forma activa en el conflicto. Por ejemplo, un individuo, que movido por un sentimiento de odio, prepara un IED y lo coloca al paso de una patrulla. En este caso su intervención comprendería desde que prepara la bomba hasta que vuelve a su domicilio.

De la misma manera puede ocurrir con los ciberataques. Así, un hacker puede preparar un virus para ser introducido en el sistema informático que controla los procesos de una planta de depuración de aguas y que, al cabo de unos días, provoque muertos por envenenamiento entre la población. El inicio de la participación directa lo definiría el momento en que empieza a diseñar el virus informático, sin embargo el final no queda claro. Se podría decir que acaba cuando lanza el virus, aunque los efectos se manifiesten después. Cabe también

preguntarse si se le podría atacar, en el momento de conocer los efectos, aunque haya pasado ya un tiempo.

La mayoría del GIE acordó que los civiles retienen su estado civil, incluso si participan directamente en las hostilidades cibernéticos. Otros, como T. Ruys afirman que una vez han cesado sus actividades, habrían recuperado su estatus de civiles y sólo cabría detenerles y en ningún momento podrían ser atacados[38].Sin embargo, podríamos estar ante un abuso flagrante del estatuto de personas civiles[39].

**Conclusiones**

Las TIC, en su aplicación al ciberespacio, han contribuido enormemente a la globalización y han supuesto una gran revolución en nuestra forma de vida. Los progresos y comodidades que nos ha traído el ciberespacio han hecho que se conciba como un "lugar" donde las variables espacio y tiempo no se contemplan.

Pero estos logros sumados a la ausencia de fronteras y la dificultad de localización de los autores de un hecho; han favorecido que los delincuentes y terroristas estén contemplando al ciberespacio como "su paraíso" donde trasladarse para continuar con gran impunidad sus fechorías.

A lo largo de este trabajo se ha visto que, frente a un uso malvado del ciberespacio, existe un vacío legal sobre ciertos usos en la red y que por tanto hay que regularlo desde el equilibrio en los principios de libertad y seguridad. La autorregualción no cumple las expectativas a largo plazo y puede ser una solución, en tanto en cuanto, los Estados y la Comunidad Internacional, a través de expertos juristas y relacionados con las TIC, puedan alcanzar acuerdos globales.

El ciberespacio, como "bien de interés público global", requerirá de normas que sean aprobadas con el mayor consenso. La seguridad en el ciberespacio no se limita a un mero aspecto técnico de la misma, sino que sobre él descansan importantes pilares de la economía y la seguridad de una nación. Además no es un problema sólo del Estado ya que un gran número de infraestructuras críticas son controladas por las empresas privadas y esto provoca que la seguridad informática sea una de sus máximas preocupaciones debido a que son depositarias de un gran número de aspectos que conforman el puzzle del bienestar de los ciudadanos.

En las relaciones internacionales también el ciberespacio juega un papel destacable, configurándose como un nuevo escenario de confrontación. La ciberguerra parece confirmarse como una nueva forma de llevar a cabo un conflicto, a tenor de los hechos conocidos (Estonia, Stuxnet, etc) y de las respuestas de los gobiernos (Computer Emergency Response Team (CERT), ciberejercitos, etc.). Pero también puede ser un recurso de actores, estatales y no estatales, ante un enemigo superior en armamento convencional, ayudando a

completar el concepto de "asimetría". Así, ésta podría ser una de las causas de que se vea con dificultad llegar a un consenso en esta materia.

Ante esta falta de voluntad nos podemos ver ante un conflicto y sobre el que trataremos de aplicar el DIH. Una solución a este problema ha sido el Manual de Tallín que no hace más que confirmar que, si difícil era en muchos casos aplicar la Carta y el DIH a los conflictos convencionales, ahora las características intrínsecas del ciberespacio; no hace más que complicar más el asunto y ahondar más en el problema.

Desde una breve interpretación de la aplicación del DIH a la ciberguerra , se ha podido constatar que existen importantes problemas pendientes: La dificultad de identificar actores y responsabilidades, el uso de la fuerza y la legítima defensa basada en los efectos, el problema de saber diferenciar bienes de interés civil y militar ante la interconexión de la red, la participación directa en las hostilidades en la ciberguerra, entre otras; no hacen más que corroborar la sensación de falta de legislación.

El mayor reto que tienen los juristas es tratar de ordenar el uso pacífico de todos aquellos avances tecnológicos para evitar así un mal uso del ciberespacio. El tiempo pasa y la no experiencia empírica de un ciberataque con consecuencias físicas pudiera no estar tan lejos en el tiempo.

Jesús Reguera Sánchez *es comandante del Ejército de Tierra y Máster en Estudios Estratégicos y Seguridad Internacional por la Universidad de Granada*

**Bibliografía**

"Agenda digital para Europa". Síntesis de la legislación de la EU. [Citado 27 de abril de 2014]): disponible en http://europa.eu/legislation_summaries/information_society/strategies/si0016_es.htm

Ahijado, Celia. "El primer manual de ciberguerra por encargo de la OTAN". ALTICNATIVA, (26 marzo de 2013[citado 3 de mayo de 2014]): disponible en http://www.lahuelladigital.com/alticnativa/el-primer-manual-de-ciberguerra-por-encargo-de-la-otan/

Andrades, Fran. "Cinco escenarios de ciberguerra en el nuevo orden mundial". Diario Turing, (7 de mayo de 2013 [citado 4 de mayo de 2014]): disponible en http://www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden_mundial_0_129837338.html

Barat-Ginies, Oriane. "Informe jurídico del CCD CoE-El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra-Informe final a 22 de noviembre de 2012", trad. Gabinete de Traductores e intérpretes del Estado Mayor del Ejército de Tierra (Madrid, 2013, traducción nº 13-0623).

Chernenko Elena, "Rusia teme que la OTAN haya desarrollado un documento para legitimar las ciberguerras". Rusia beyond de headlines, (28 de mayo de 2013 [citado 10 de mayo de 2014]): disponible en http://es.rbth.com/cultura/technologias/2013/05/28/rusia_teme_que_la_otan_haya_desarrollado_un_documento_pa_28313.html

"Ciberguerra el nuevo campo de batalla para las empresas".Cronista.com, (8 de febrero de 2011 [citado 9 de mayo de 2014]): disponible en http://www.cronista.com/itbusiness/Ciberguerra-el-nuevo-campo-de-batalla-para-las-empresas-20110208-0010.html

Del derecho y las Normas. (23 de junio de 2010 [citado 14 de mayo de 2014]): disponible en http://derechoynormas.blogspot.com.es/2010/06/reforma-del-codigo-penal-delitos.html

"Cybercrimen". e-boletín legal de Derecho Penal Informático, nº1 (septiembre 2012) [citado 25 de abril de 2014]): disponible en http://www.iriartelaw.com/sites/default/files/boletincc-anoI-n1-2012_0.pdf

Consigly, Lavopa:"Dos aspectos de la Legítima Defensa frente a la amenaza terrorista" Derecho internacional.net, ),[citado 15 mayo de 2014]): disponible en http://www.derechointernacional.net/publico/fuentes-normativas-generales/parte-especial/277-consigli--lavopa-dos-aspectos-de-la-legitima-defensa-frente-a-la-amenaza-terrorista-.html

Código Penal (artículos relativos a Delitos informáticos), [citado 14 mayo de 2014]): disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/normativa_estatal/common/pdfs/E.2-cp--C-oo-digo-Penal.pdf

Cuadernos de Estrategia. Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio. Madrid. Ministerio de Defensa, 2011.

Dans, Enrique, "Sobre anonimato y redes sociales". El blog de Enrique Dans (06 agosto 2011) [citado 26 de abril de 2014]): disponible en http://www.enriquedans.com/2011/08/sobre-anonimato-y-redes-sociales.html

Droege, Cordula, "No hay lagunas jurídicas en el ciberespacio". CICR Entrevista, (16 de agosto de 2011 [citado 1 de mayo de 2014]): disponible en http://www.icrc.org/spa/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

Guzman, Rosa. "El uso del ciberespacio: consideraciones éticas y legales". Cuaderno de Investigación en la Educación, número 21 (diciembre 2006) [citado 23 de abril de 2014]): disponible en http://cie.uprrp.edu/cuaderno/ediciones/21/06.html

Herrera, Rodolfo, "Ciberespacio, sociedad y derecho". Revista chilena de Dercho Informático, [citado 23 de mayo de 2014]): disponible en http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10664/10946

"Internet: Un espacio para el cibercrimen y el ciberterrorismo". IV Congreso de Cibersociedad 2009, (27-29 de noviembre de 2009 [citado 24 de abril de 2014]): disponible en http://www.cibersociedad.net/congres2009/es/coms/internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo/610/

Ibarra, Jessica G. "Seguridad Cibernética". Foreign Affairs Latinoamérica, [citado 16 de abril de 2014]): disponible en http://www.revistafal.com/index.php?option=com_content&view=article&id=586:seguridad-cibernetica-en-el-mundo-y-latinoamerica&catid=156&Itemid=490

Jordán, Javier y Calvo José Luís. El nuevo rostro de la guerra. Pamplona. Ediciones Universidad de Navarra, S.A, 2005.

Jodan, Javier (coords). Manual de estudios estratégicos y seguridad internacional. Plaza y Valdes Editores, 2013.

Klimberg, Alexander. NationaL Cyber Security Framework Manual. Tallinn. NATO CCD COE Publication, 2012.

"La ciberguerra es inevitable". Un lugar para la ciencia y la tecnología, mi+d, (5 de junio de 2013 [citado 7 de mayo de 2014]): disponible en http://www.madrimasd.org/informacionidi/noticias/noticia.asp?id=56989

"La OTAN publica manual de ciberguerra". DiarioTi.com - el diario del profesional TI, (21/03/13[citado 3 de mayo de 2014]): disponible en http://diarioti.com/la-otan-publica-manual-de-ciberguerra/62351

López, Paula. El Ciberespacio y su Ordenación. Madrid. Grupo Difusión: Difusión Jurídica y Temas de Actualidad, S.A, 2006.

Mazo, Angel, "La Ciberseguridad en el contexto de la OTAN y la UE". Ponencia del XXVI Curso de verano - Universidad Complutense Madrid (julio de 2013) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, citado 22 de abril 2014]): disponible en http://www.ieee.es/Galerias/fichero/cursosverano/ElEscorial2013/Ciber_Escorial_Mazo.pdf

Miró, Fernando. El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid. Marcial Pons, 2012 [citado mayo de 2014]): disponible en https://www.marcialpons.es/static/pdf/9788415664185.pdf

Monografías del CESEDEN. Los Ámbitos no Terrestres en la Guerra Futura: Espacio. Ministerio de Defensa, 2012.

Prieto, Ramón. Guerra cibernética: Aspectos organizativos Grupo de Trabajo nº 3 XXXIII Curso de Defensa Nacional, abril 2013 [citado 26 de mayo de 2014]): disponible en http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

Rauscher, Karl. "Ciberguerra: es hora de escribir sus reglas". Prueba & Error, (20 de diciembre de 2013 [citado 9 de mayo de 2014]): disponible en http://www.pruebayerror.net/2013/12/ciberguerra-es-hora-de-escribir-sus-reglas/

Ricaurte, Paola. "Cibercrimen: El nuevo rostro de la delincuencia". Mediosfera. Reflexiones acerca de los medios y la sociedad, (24 de septiembre de 2009 [citado 24 de abril de 2014]): disponible en http://mediosfera.wordpress.com/2009/09/24/cibercrimen-el-nuevo-rostro-de-la-delincuencia/

Rizzi, Andrea. "La línea Maginot de la ciberguerra". El país, (2 de noviembre de 2009 [citado 4 de mayo de 2014]): disponible en http://elpais.com/diario/2009/11/02/internacional/1257116403_850215.html

Segura, Antonio y Fernando Gordo, (coords.). Cibereseguridad Global. Granada. Universidad de Granada, 2013.

Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed". Harvard international law journal, (diciembre 2012 [citado 10 de mayo de 2014]): disponible en http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf

Tallinn Manual of the International Law applicable to Ciberwarfare. Cambridge. Cambridge University Press, [2013, citado 01 mayo de 2014]): disponible en https://ia801703.us.archive.org/22/items/TallinnManual/TallinnManual.pdf

Molina, José M. Ciberseguridad y Derecho (varios documentos), disponible en http://molinamateos.com/content/legislaci%C3%B3n

Resolución de las NNUU, [2006, citado 14 mayo de 2014]): disponible en http://www.itu.int/newsroom/wtd/2006/pdf/UNGA_57-239-es.pdf
http://www.itu.int/newsroom/wtd/2006/Pdf/UNGA_58-199-es.pdf

Touré, Hamadoun. La búsqueda de la Paz en el Ciberespacio. Ginebra. División de Estrategia de la Unión Internacional de Telecomunicaciones. Ginebra. ITU,[2011, citado 25 mayo de 2014]): disponible en http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-S.pdf

---

[1] Ciberespacio: Dominio global y dinámico compuesto por infraestructuras de tecnología de la información —incluyendo Internet—, redes de telecomunicaciones y sistemas de información (BOD Nº40 23FEB13, Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

[2] "Internet: Un espacio para el cibercrimen y el ciberterrorismo", *IV Congreso de Cibersociedad 2009"* [consultado abril 2014]: disponible en http://www.cibersociedad.net/congres2009/gl/coms/internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo/610/

[3] P. López Zamora, "El ciberespacio y su ordenación", Capítulo 2: Regulando el ciberespacio (Difusión jurídica y temas de actualidad, 2006) citando a Graham G, "*Internet, una indagación filosófica",* pp 94-95. [consultado abril 2014]: disponible en http://www.difusionjuridica.com.bo/bdi/biblioteca/biblioteca/libro094/lib094-2.pdf

[4] Apuntes Ponencia: La ética ante los dilemas de la globalización. " XXVI Curso de Verano Universidad Complutense: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio" julio 2013.

[5] F. Savater, El límite ético, "Atenea", nº 49, (septiembre 2013):26.

[6] El phishing es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de

crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta http://seguridad.internautas.org/html/451.html

[7] Los Troyanos Informáticos o Caballos de Troya (en inglés Trojan) es una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos legítimos/benignos (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño. http://www.seguridadpc.net/troyanos.htm

[8] Malware es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. http://www.infospyware.com/articulos/que-son-los-malwares/

[9] El cibercrimen generó unas pérdidas de 87.000 millones de euros en todo el mundo entre noviembre del 2012-2013 y se ha convirtiéndose en «uno de los negocios más lucrativos que no ha sufrido la crisis». http://www.abc.es/tecnologia/redes/20131105/abci-cibercrimen-millones-perdidas 201311052029.html

[10] Wael Adhami, La importancia estratégica de Internet para los grupos armados insurgentes en las guerras modernas, *"International revue of the Red Cross"*, (diciembre 2007):306.

[11] J.S Nye, Ciberguerra y ciberpaz, "Project Syndicate": [consultado mayo 2014]:disponible en http://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish

[12] BOD Nº40 23FEB13, Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas españolas.

[13] A. Segura y F. Gordo (coords), Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio (Granada: Universidad de Granada, 2013), 45.

[14] R. Gil Navalón, El vacío legal del ciberespacio, *"Revista de Aeronáutica y Astronáutica"*, (octubre 2012):849.

[15] P. López Zamora, "El ciberespacio y su ordenación", Capítulo 2: Regulando el ciberespacio (Difusión jurídica y temas de actualidad, 2006):95.[consultado abril 2014]: disponible en http://www.difusionjuridica.com.bo/bdi/biblioteca/biblioteca/libro094/lib094-2.pdf

[16] M. Díaz de Terán, "Lecciones de Teoría Del Derecho" (Universidad de Navarra Curso académico 2013/2014):18.

[17] Ciberespacio. Sobre la "Declaración de Independencia del Ciberespacio", [consultado junio 2014]: disponible en http://ciberpolitik.awardspace.com/independencia.htm

[18] M. Díaz de Terán, "Lecciones de Teoría Del Derecho" (Universidad de Navarra Curso académico 2013/2014):19.

[19] P. López Zamora, "El ciberespacio y su ordenación", Capítulo 2: Regulando el ciberespacio (Difusión jurídica y temas de actualidad, 2006), 104, citando a Asensio P., "Derecho Privado de Internet" (Civitas, Madrid,2000), 76. [consultado junio 2014]: disponible en http://www.difusionjuridica.com.bo/bdi/biblioteca/biblioteca/libro094/lib094-2.pdf

[20] E. Suñé Llinás, "Declaración de Derechos del Ciberespacio", El ciberespacio y las generaciones de derechos, [consultado abril 2014]: disponible enhttp://portal.uexternado.edu.co/pdf/7_convencionesDerechoInformatico/documentacion/conferencias/Los_Derechos_Humanos_en_el_Ciberespacio.pdf

[21] P. López Zamora, "El ciberespacio y su ordenación", Capítulo 2: Regulando el ciberespacio (Difusión jurídica y temas de actualidad, 2006):128 [consultado abril 2014]: disponible en http://www.difusionjuridica.com.bo/bdi/biblioteca/biblioteca/libro094/lib094-2.pdf

[22] Cooperación Jurídica Internacional. Orden Europea de Detención y Entrega, [consultado junio 2014]: disponible en http://www.mjusticia.gob.es/cs/Satellite/es/1215197995954/Tematica_C/1215198003700/Detalle.html

[23] Mision and vision CCD COE, [consultado mayo 2014]: disponible en http://www.ccdcoe.org/11.html

[24] Oriane Barat-Ginies, "Informe jurídico del CCD CoE-El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra-Informe final a 22 de noviembre de 2012", trad. Gabinete de Traductores e intérpretes del Estado Mayor del Ejército de Tierra (Madrid, 2013, traducción nº 13-0623) pag. 15.

[25] T. Gjelten, "Extending The Law Of War To Cyberspace", [septiembre 2010, consultado junio 2014]: disponible en http://www.npr.org/templates/story/story.php?storyId=130023318

[26] Oriane Barat-Ginies, "Informe jurídico del CCD CoE-El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra-Informe final a 22 de noviembre de 2012", trad. Gabinete de Traductores e intérpretes del

Estado Mayor del Ejército de Tierra (Madrid, 2013, traducción nº 13-0623) pag 28.

[27] Las Infraestructuras cibernéticas hacen referencia a las comunicaciones, almacenaje y recursos informáticos con los que los sistemas de información operan. Oriane Barat-Ginies, "Informe jurídico del CCD CoE-El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra-Informe final a 22 de noviembre de 2012", trad. Gabinete de Traductores e intérpretes del Estado Mayor del Ejército de Tierra (Madrid, 2013, traducción nº 13-0623) pag 22.

[28] Artic. 8 de la Resolución aprobada por la Asamblea General 56/83 delas NNUU (28-1-82) "Responsabilidad del Estado por hechos internacionalmente ilícitos"

[29] Artic. 16 y 17 de la Resolución aprobada por la Asamblea General 56/83 delas NNUU (28-1-82) "Responsabilidad del Estado por hechos internacionalmente ilícitos".

[30] Artic. 49.3 de la Resolución aprobada por la Asamblea General 56/83 delas NNUU (28-1-82) "Responsabilidad del Estado por hechos internacionalmente ilícitos".

[31] Artic. 50.1 c) y 51 de la Resolución aprobada por la Asamblea General 56/83 delas NNUU (28-1-82) "Responsabilidad del Estado por hechos internacionalmente ilícitos".

[32] Artic. 50.1 a) de la Resolución aprobada por la Asamblea General 56/83 delas NNUU (28-1-82) "Responsabilidad del Estado por hechos internacionalmente ilícitos".

[33] Artic. 59 de la Resolución aprobada por la Asamblea General 56/83 delas NNUU (28-1-82) "Responsabilidad del Estado por hechos internacionalmente ilícitos".

[34] Tallinn Manual of the International Law applicable to Ciberwarfare (Cambridge University Press, 2013): 49-52 [consultado 15 junio de 2014]): disponible en https://ia801703.us.archive.org/22/items/TallinnManual/TallinnManual.pdf

[35] J. Flores Artículos. Stuxnet y el nacimiento de la ciberguerra, [2013, consultado junio 2014]: disponible en http://www.qore.com/articulos/6560/Stuxnet-y-el-nacimiento-de-la-ciberguerra

[36] Oriane Barat-Ginies, "Informe jurídico del CCD CoE-El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra-Informe final a

22 de noviembre de 2012", trad. Gabinete de Traductores e intérpretes del Estado Mayor del Ejército de Tierra (Madrid, 2013, traducción nº 13-0623) pag 33.

[37] Díaz Barrado y Fernández Liesa, Derecho Internacional humanitario y Derechos Humanos, (eds.). J.L. Rodríguez Villasante. Targeted Killing: de los ataques letales selectivos y a las ejecuciones extrajudiciales capítulo 12 p. 374.

[38] T. Ruys, License to kill? State-sponsored assassination under international law, en Revista de Derecho Militar y de Derecho de Guerra, nº44, 2005, Vol 1-2, p. 29

[39] Díaz Barrado y Fernández Liesa, Derecho Internacional humanitario y Derechos Humanos, (eds.). J.L. Rodríguez Villasante. Targeted Killing: de los ataques letales selectivos y a las ejecuciones extrajudiciales capítulo 12 p. 377.