CIBERSEGURIDAD GLOBAL

OPORTUNIDADES Y COMPROMISOS EN EL USO DEL CIBERESPACIO

Antonio Segura Serrano
Fernando Gordo García
(Coords.)

CIBERSEGURIDAD GLOBAL

OPORTUNIDADES Y COMPROMISOS EN EL USO DEL CIBERESPACIO

GRANADA
2013

El Centro Mixto UGR-MADOC no se responsabiliza de las opiniones de los autores

CIBERSEGURIDAD GLOBAL. OPORTUNIDADES Y COMPROMISOS EN EL USO DEL CIBERESPACIO
ISBN: 978-84-338-5600-5 Depósito legal: Gr./2.117-2013
Edita: Editorial Universidad de Granada
Campus Universitario de Cartuja. Granada
Fotocomposición: García Sanchis, M.J., Granada
Diseño de cubierta: José María Medina Alvea
Imprime: Imprenta Comercial. Motril. Granada
Printed in Spain *Impreso en España*

INDICE

PARTE III
TECNOLOGÍAS DE IMPARABLE PROGRESIÓN EN EL CIBERESPACIO. INVESTIGACIÓN, PREPARACIÓN Y RETOS EN MATERIA DE CIBERDEFENSA MILITAR

Parte IV
EL CAMINO HACIA UNA CIBERSEGURIDAD INTEGRAL EN ESPAÑA

PRÓLOGO [1]

ALFREDO RAMÍREZ FERNÁNDEZ

El imparable progreso y utilización de las tecnologías de la información y las telecomunicaciones (TIC) en todas las esferas sociales, ha conformado una nueva dimensión donde interactuar y a la que se le ha denominado ciberespacio. Las tradicionales áreas donde nos relacionábamos hace muy poco tiempo, insignificante en relación con la historia de la humanidad, eran la tierra, el mar, el aire y el espacio. En todos ellos se han forjado increíbles avances que han impulsado la prosperidad de las sociedades. Sin embargo, debemos admitir que sobre todo los tres primeros, también han sido lamentablemente los escenarios de innumerables conflictos armados que han hecho retroceder o despedazar las esperanzas y las ilusiones de muchos seres humanos.

El ciberespacio, como elemento común y global que puede expandirse sin límites, está repleto de oportunidades de prosperidad pero al mismo tiempo de vulnerabilidades. El sector de la seguridad y la defensa en todas las naciones democráticas y libres, adquiere por tanto un protagonismo y responsabilidad vital para ser capaces de prepararse técnicamente y aplicar en todos estos espacios las lecciones aprendidas que impidan agresiones a la seguridad nacional, al estado de derecho, al bienestar de la ciudadanía, a la economía, y en definitiva, al normal funcionamiento de todos los sectores de la nación.

Junto a este vertiginoso progreso repleto de avances tecnológicos, se han visto catalizados al unísono y de una forma sin precedentes, las relaciones sociales y los procesos de toma de decisiones que ven a la inmediatez y a la disponibilidad de grandes volúmenes de información al instante en todo tipo de dispositivos fijos

1. Alfredo Ramírez Fernández es Teniente General del Ejército de Tierra y Jefe del Mando de Adiestramiento y Doctrina. Granada.

y móviles, como características relevantes. Millones de personas los utilizan cada segundo para realizar actividades profesionales y personales de cualquier naturaleza en este nuevo mundo digital, el ciberespacio.

La ciberseguridad será una responsabilidad esencial de todos los actores que interactúan en este nuevo entorno compuesto por todo tipo de redes y tecnologías donde se mueve la información sin barreras, tanto nacional como internacionalmente. Legisladores, decisores políticos, militares, proveedores de TIC, investigadores, docentes, etc., encuentran en el ciberespacio muchas de las respuestas o recomendaciones a las mismas que sería inimaginable poder obtener en épocas pasadas. Pero esa facilidad no debe confundirnos ni desviar la atención de las cuestiones relevantes para la seguridad y la defensa requiriendo inexcusablemente que su empleo deba ser regulado y asegurado.

Es necesario seguir trabajando de una forma responsable y colectiva para alcanzar las soluciones y mejores prácticas que mitiguen en todo lo posible las amenazas en el ciberespacio, no sólo aquellas que pueden tener efectos físicos contra infraestructuras críticas o contra los sistemas de información. Los efectos resultantes de la gestión de las percepciones en este espacio cibernético, pueden resultar incluso con efectos más contundentes transformando sociedades, conductas y formas de vida.

No resultaría comprensible ni eficaz, para mantener nuestros intereses, trabajar aislados o compartimentando tecnología, leyes o ciencias sociales, en este complejo entorno. En consecuencia, se debe reconocer el esfuerzo de muchos de los sectores de la sociedad que trabajan en beneficio de la seguridad intentando cuantificar y valorar las amenazas para neutralizarlas en lo posible desde sus ámbitos de actuación respectivos pero manteniendo una visión común global.

A pesar de las limitaciones de nuestra contribución desde la metodología de la investigación y la experimentación de conceptos, en una perfecta sintonía entre civiles y militares, es indudable que este trabajo agregará valor a otros esfuerzos en curso, sirviendo de un instrumento más de utilidad para generar recomendaciones en beneficio de una mayor ciberseguridad global. Este libro que se complace de un enfoque integral, ha contado

con la cooperación, entusiasmo y esfuerzo de muchos de ellos, a los que dirijo desde estas líneas mi sincero agradecimiento como Director de Investigación, Doctrina, Orgánica y Materiales del Mando de Adiestramiento y Doctrina del Ejército de Tierra, en el momento de su redacción y como responsable de las actividades relacionadas con el mismo dentro del innovador Programa de Investigación sobre Ciberdefensa. La universidad, la empresa, el área de la seguridad y la defensa, y el resto de actores que han colaborado, sin duda han compartido y demostrado su voluntad responsable por los intereses de España, y el firme compromiso por la seguridad de todos.

AGRADECIMIENTOS

Ciberseguridad Global. Oportunidades y compromisos del uso del Ciberespacio, es el título dado al trabajo que el lector podrá examinar a continuación del que se puede destacar el carácter innovador del amplio programa de investigación (PINV) en el que se enmarca. Dentro de ese PINV, una de las actividades iniciales de carácter docente y de apoyo a la investigación al mismo tiempo, consistió en desarrollar un completo curso académico de carácter teórico y práctico sobre ciberseguridad, —que llevó por nombre: *Ciberseguridad, oportunidades para trabajar y contribuir a la seguridad de todos*—, contando con un seleccionado grupo de profesores del ámbito militar y civil que se dieron cita durante la semana del 18 al 20 de septiembre de 2012 en las instalaciones del Centro Mediterráneo del complejo Triunfo de la Universidad de Granada.

Desde el ámbito de Defensa participaron conferenciantes de la Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del MADOC, de la Jefatura de Telecomunicaciones, Sistemas de Información y Asistencia Técnica (JCISAT) del Cuartel General del Ejército de Tierra, del Área de Telecomunicaciones y Ciberseguridad del Instituto Tecnológico de la Marañosa (ITM) de la Dirección General de Armamento y Material (DGAM), del Grupo de Delitos Tecnológicos (GDT) de la Guardia Civil, y del Centro Criptológico Nacional (CCN) del Ministerio de la Presidencia.

Del ámbito Académico se contó con profesores procedentes de Universidades españolas como la de Granada, con el Centro de Investigación de las Tecnologías de Información y Comunicaciones (CITIC), y la Facultad de Derecho (Dpto. Dcho. Internacional Público y RRII, y Dpto. Dcho. Penal), de las Universidades Autónoma (Dpto. Dcho. Internacional Público), y Politécnica (Escuela Técnica Superior de Ingenieros de Informática y de Telecomunicación, ETSIIT) de Madrid, de la Universidad de Bar-

celona Pompeu Fabra (Dpto. Relaciones Internacionales), y de la prestigiosa Universidad *The College of William & Mary*, Virginia (Estados Unidos).

Del Ministerio Fiscal colaboró el servicio de Cooperación Internacional y delitos informáticos de la Fiscalía Provincial de Granada, y del sector privado hay que destacar la activa colaboración de las empresas españolas S21sec y *Voice Consulting*, tanto en la parte teórica como en la práctica de los talleres.

El excelente análisis, desde una perspectiva global nacional e internacional, ofrecido por todos los expertos españoles de primer orden que formaron el amplio equipo multidisciplinar docente, sirvió para establecer eficazmente una buena parte de las bases teóricas del PINV y, en particular, del concepto teórico resultante. Las conclusiones y recomendaciones principales de muchos de ellos, además de haber quedado reflejadas en esta publicación, sirvieron para enriquecer un concepto sólido sobre ciberseguridad y ciberdefensa que se experimentaría sólo tres meses después.

Los laboratorios y personal de ciberseguridad del Instituto Tecnológico de la Marañosa (ITM) en San Martín de la Vega (Madrid)-, colaboraron eficazmente con el Ejército de Tierra a través del MADOC en tal misión. En suma, un detallado, innovador, y completo planeamiento de investigación aplicando el método científico conocido en OTAN como proceso de *Concept Development & Experimentation* (CD&E), que permitió obtener productos en beneficio de la seguridad.

Resulta de justicia agradecer a todos los ponentes del curso de ciberseguridad de Granada sus aportaciones al mismo, así como reconocer el esfuerzo y profesionalidad demostrado por todos. Algunas cuestiones podrán ser completadas en publicaciones posteriores como los asuntos relacionados con el estado en el que se encuentra la ciberdelincuencia a nivel global, analizado desde un prisma eminentemente práctico basado en las investigaciones del Grupo de Delitos Telemáticos de la Guardia Civil, la forma de actuación del Ministerio Fiscal, introduciendo los fundamentos sociológicos subyacentes a las nuevas amenazas terroristas enlazadas con las tecnologías de la información.

Todo ello dentro del constante análisis del marco legal de respuesta, tanto preventiva como criminal, al fenómeno del ciberter-

rrorismo. De las conclusiones expuestas quedan igualmente líneas de investigación abiertas referentes a los instrumentos normativos e institucionales que debe obtener España para la respuesta preventiva y reactiva frente a los ataques ciberterroristas tanto para la referida protección de infraestructuras críticas, como para las actividades de investigación e inteligencia, prevenciones penales, la competencia de los órganos judiciales nacionales, y la imprescindible cooperación judicial internacional.

De cualquier forma y gracias al éxito del resultado del PINV, tanto por la calidad del curso gracias a sus docentes, moderadores, organizadores, la cantidad y activa participación de sus alumnos, como posteriormente por el desarrollo del primer ejercicio experimental nacional de ciberdefensa que ha constituido un importante hito de esta materia en España, como así reflejaron muchos medios, se puede afirmar sin dilación que una vez más el CEMIX ha dejado buena constancia de aquellos valores que inspiraron su creación, desprendidos en enérgica sintonía desde ambas instituciones en Granada, el MADOC y la UGR.

El ciberespacio aceptado como un dominio global y común de actuación; el análisis, en términos de sus implicaciones para la seguridad y la defensa, sobre cómo obtener una ciberdefensa eficaz y eficiente en cuanto a organización, estructura, instrumentos, capacidades y misiones; la necesidad de completar una legislación y un marco jurídico comprensible y consensuado nacional e internacionalmente; la implicación del sector empresarial privado y sus responsabilidades en cuanto a las tecnologías duales en permanente interacción con la seguridad y la defensa; y la imperante necesidad de dotar especialmente a nuestros jóvenes y profesionales de una educación estructural en el ciberespacio han sido, entre otros, algunos de los temas que nuestra investigación ha pretendido desarrollar y que quedan reflejados de alguna forma a través de las aportaciones de los coautores de esta obra.

A todos ellos, una vez más, va dirigido el agradecimiento por su valioso aporte científico a la seguridad.

INTRODUCCIÓN

Fernando Gordo García[1]
Antonio Serrano Segura

El día trece de diciembre del año 2011, los responsables de la Comisión Mixta constituida entre la Universidad de Granada (UGR) y el Mando de Adiestramiento y Doctrina (MADOC) del Ejército de Tierra (ET), aprobaban en su reunión número quince, el Plan Anual de Colaboración previsto para el siguiente año (PAC 2012). Paralelamente en aquellos momentos, se estaban dando los primeros pasos para constituir el principal elemento operativo del Centro Mixto (CEMIX) entre dichas instituciones sitas en la ciudad de Granada, nos referimos a su Unidad de Investigación (UINV).

Esta unidad acababa de organizarse pocos meses antes sobre la base de tres áreas de investigación prioritarias donde se emplazaron dos responsables investigadores por cada una de ellas; uno civil de reconocido prestigio investigador por la UGR, nombrado por el Consejo de Dirección con la conformidad del Vicerrectorado de Investigación, y uno militar analista con experiencia por parte del MADOC, concretamente designado por su Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM).

Así, acudiendo a la terminología militar, las unidades de maniobra investigadoras quedaron constituidas por el CEMIX en julio de 2011; línea número uno: *Escenarios actuales y potenciales de conflicto relacionados con la seguridad*, línea número dos: *Ayuda a la toma de decisiones*, y línea número tres: *La Historia como fuente de lecciones aprendidas (recientemente transformada en Cultura y Sociedad).*

Conscientes del trascendente compromiso que ostentaban, sus responsables empezaron de inmediato a trabajar motivados al mismo tiempo por el ilusionante reto que se presentaba. Se debe no obstante destacar, que no empezaban desde cero puesto

1. Fernando Gordo García, fue, junto con Antonio Segura Serrano, el director del Curso de Verano sobre Ciberseguridad de la Universidad de Granada, realizado en septiembre de 2012 en el Centro Mediterráneo de dicha universidad.

que recordemos que el CEMIX fue creado dentro del marco del convenio de colaboración entre la Universidad de Granada y el Ministerio de Defensa de 19 de julio del año 1994. Seguidamente a la hora de organizar la estructura del MADOC, la colaboración con la universidad se consideró primordial para el cumplimiento de sus misiones y para ello se estimó clave promover el desarrollo de una cultura de diálogo y cooperación continuada y sistemática.

Una cooperación con objetivos prácticos entre la UGR y el MADOC, y entre ellos y todos los actores implicados en el desarrollo teórico y aplicado de las ciencias aspirando a constituir un referente en la generación de conocimiento orientado a la resolución de los problemas prácticos que afectan a las instituciones y entidades que trabajan por la seguridad, la defensa y la construcción de la paz.

El prestigio y las características singulares de la UGR, fueron factores importantes en la elección de la ciudad de Granada como sede principal del MADOC, conformando algunos de los elementos cardinales para desarrollar de forma eficiente las actividades de este Mando, en especial las relacionadas con la inseparable terna formada por la investigación, las lecciones aprendidas y la doctrina. Conjunto básico éste para apoyar al sistema de preparación de las fuerzas terrestres que debía contar con el riguroso apoyo académico que le proporcionase un carácter práctico e innovador a la hora de mantenerse al día de los avances y cambios sociales, culturales, científicos, tecnológicos, etc., del incierto y complejo entorno operativo en el que se desenvuelven las actuaciones de nuestras Fuerzas Armadas.

La Comisión Mixta, creada el 17 de marzo de 1998, constituyó así el inicio oficial de una colaboración constante hasta hoy desarrollando anualmente los PAC, uno por curso académico, contemplando un amplio elenco de actividades dentro del denominado enfoque integral en las áreas principales de formación, organización y enlace, investigación e innovación y servicios. Para terminar este repaso histórico concluiremos diciendo que entre esas actividades, en este caso reflejada en el PAC 2012 citado al comienzo de esta introducción, se encuentra la que da origen a esta obra que ahora se presenta, *Ciberseguridad Global. Oportunidades y compromisos del uso del Ciberespacio.*

Este libro está estructurado en cuatro partes. La primera de ellas ofrece de forma magistral el marco introductorio a la situación global de seguridad en el contexto de los conflictos armados actuales. Este análisis introductorio realiza un breve examen de los conceptos de seguridad y defensa e indaga en la mayor internacionalización y privatización que están experimentando los recientes conflictos armados. Asimismo, desde el marco de un concepto amplio de seguridad internacional, se presta especial importancia a distintos aspectos claves tales como la economía, los derechos humanos o los nuevos perfiles de las fuerzas armadas.

La segunda parte está orientada a arrojar algo de luz, bajo un riguroso estudio, sobre algunas de las cuestiones más relevantes con que se enfrentan aquellos que consideran trascendental regular el uso del ciberespacio y en particular de Internet. Desde una inescapable visión *iusinternacionalista*, el lector podrá profundizar sobre cuestiones de plena actualidad relacionadas con el ciberespacio. En primer lugar, surge la problemática relativa a si es posible y legítimo someter a regulación las actividades que se desarrollan en Internet, así como la concerniente a la gobernanza de la Red. Además, se tratan extensamente problemas de amplio alcance jurídico, como el derecho a la privacidad, la restricción del acceso a ciertos contenidos, la propiedad intelectual, otros potenciadores del riesgo en el ciberespacio como la bioseguridad, así como algunas consideraciones políticas y tecnológicas también presentes, entre otras cuestiones. El uso de la Fuerza en relación con las actuaciones en el ciberespacio, recibe una especial atención en esta parte del libro puesto que posteriormente en la siguiente parte de la obra, se tratará de las capacidades necesarias para poder ejercer una ciberdefensa completa en todos sus aspectos. Bajo el enfoque de sus analistas, se asume que en los últimos tiempos Internet se ha convertido en un elemento que permite ocasionar perjuicios a servicios estatales básicos de los que pueden resultar, aunque sea temporalmente, efectos equivalentes a los que produciría el uso de la fuerza armada. La aportación de este análisis nos llevará a reflexionar acerca de en qué medida y circunstancias podemos considerar esos ataques informáticos como un uso de la fuerza, identificando las dificultades de hacerlo, así como las posibles reacciones a esas amenazas actuales.

Todo ello sin dejar de lado las posibles respuestas, siempre desde la seguridad jurídica en la esfera universal global y común, con el propósito de completar los términos dentro de los cuales se producirían.

Así, la tercera parte, de corte más tecnológico y dirigida fundamentalmente a la ciberdefensa militar como uno de los pilares actuales cardinales y, sin embargo, de más corta historia de la seguridad, pretende acercar al lector al conocimiento y concienciación sobre la necesidad de que se dediquen esfuerzos convergentes desde todos los sectores de la nación tanto a la formación y preparación, como a la adquisición de medios destinados a tal fin. Entendiendo que no sólo la capacidad de defensa en sí es la única opción para garantizar la seguridad y libertad de una nación frente a actuaciones contra ella, también es inexcusable dotarse de las capacidades de explotación y respuesta en este nuevo dominio global y común de actuación que conforma el ciberespacio. Temas como la investigación, la experimentación, y su posterior aplicación práctica en beneficio de las fuerzas, así como la imparable progresión de las tecnologías duales y por ende, la expansión de sus vulnerabilidades asociadas, serán también abordadas en esta tercera parte de la obra. Se expone cómo la potenciación de la I+D+i constituye una de las mejores herramientas para estar al frente en las tecnologías de seguridad de la información y comunicaciones, STIC. Se ofrece igualmente aquí una visión sobre el seguimiento, la investigación y desarrollo de las principales tecnologías que permiten mejorar la seguridad de los sistemas de información y comunicaciones de las Fuerzas Armadas, temas como los principales retos y misiones relacionados con el ciberespacio en los que trabajan las unidades y centros dedicados a la ciberdefensa militar, el desarrollo seguro de software, los protocolos seguros, y la investigación y análisis de malware, entre otros.

La cuarta y última parte del libro, está dedicada de manos de la profesionalidad, experiencia y el conocimiento cercano, a trazar un perfil de actuación en ciberseguridad apuntando retos y prioridades desde una perspectiva española en la línea, ya indicada, del enfoque integral donde se tengan en cuenta a todos los actores de la nación, los activos críticos que deben ser defendidos, así como las estrategias necesarias para ello.

Muchos medios de comunicación reflejaron, y continúan haciéndolo frecuentemente, informaciones relativas a los temas que se podrán leer a continuación en este trabajo. Tanto el curso de Granada, como sobre todo el posterior experimento en Madrid, fueron objeto de numerosos titulares, reportajes y artículos de opinión en medios de comunicación especializados por lo novedoso del asunto. El libro que aquí se presenta, está centrado en las conclusiones del curso de Granada.

Con las limitaciones lógicas de la clasificación obligada de ciertos temas, se ha hecho un importante esfuerzo para que todas las actividades hayan gozado en general de una transparencia y flexibilidad muy valoradas por todos, facilitando así su desarrollo al contar con una notoria complementariedad de esfuerzos desde distintos sectores nacionales admitiendo un verdadero enfoque integral del asunto, el denominado comprehensive approach en terminología de la OTAN.

Por tanto, esta obra resulta de recomendada lectura para todo aquel interesado en cuestiones jurídicas, tecnológicas, o actividades de I+D en el ámbito del ciberespacio, cuya actualidad y relevancia se manifiestan especialmente en las materias de seguridad y defensa. Los estudiosos pertenecientes al ámbito académico, a las Fuerzas Armadas, la Administración Pública, instituciones, empresas, y organismos relacionados en general con la ciberseguridad encontrarán aquí una herramienta de gran utilidad.

Los recientes documentos del más alto nivel sobre seguridad y defensa, coinciden en situar a la ciberseguridad como una de las herramientas más importantes en los escenarios actuales y potenciales de conflicto futuros. El nacimiento incremental de organizaciones de distinto carácter relacionadas con la ciberdefensa en el ámbito de las principales alianzas internacionales en las que España participa, unido a los acontecimientos de actualidad que están propiciando importantes cambios sociales, económicos y políticos, estimularon al CEMIX a través de su primera línea de la UINV, para iniciar un proyecto de investigación consecuente.

Elaborado en 2010 el nuevo Concepto Estratégico de la OTAN, sancionados en el año 2011 los documentos Visión y Concepto de Ciberdefensa Militar del Jefe del Estado Mayor de la Defensa (JEMAD), y publicada por el Gobierno la Estrategia Española de Se-

guridad en junio del mismo año, ahora renovada por la Estrategia de Seguridad Nacional aprobada en mayo de 2013, el asunto de la ciberseguridad ha ido tomando un protagonismo creciente, al ser elemento común de gran parte de la sucesión de acontecimientos sociales, tecnológicos, militares, políticos y económicos que han centrado la atención institucional, académica y mediática, y de los que el CEMIX no podía quedar ajeno.

El día 7 de marzo de 2013 en el Salón del Artesonado del Acuartelamiento de la Merced del MADOC en Granada, eran presentadas oficialmente las principales conclusiones, productos y recomendaciones del PINV de Ciberseguridad y Ciberdefensa al Director de Investigación del MADOC con la asistencia de los responsables y participantes civiles y militares en el programa. Tan sólo unos días antes, la Orden Ministerial 10/2013 de 19 de febrero, ordenaba la creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, lo que certifica la constante preocupación española por la ciberseguridad.

La extensión de las tecnologías de imparable progresión relacionadas con los sistemas de telecomunicaciones e información, encuentran en el ciberespacio un escenario donde operar sin límites en el que no sólo hay que investigar la mejor preparación tecnológica de la propia defensa en su extensión más completa (defensa, explotación, y respuesta). También se debe estar en condiciones de ser capaces de delimitar el marco legal de colaboración y actuación que permita un proceso de toma de decisiones riguroso y en tiempo oportuno. De ahí, precisamente, de la complementariedad entre su carácter multidisciplinar y de su oportunidad temporal, se evidencia el marcado carácter innovador del PINV.

Desde el sentimiento de estar ante un momento crucial de la reciente historia, en el que se detecta un contexto global de crisis que afecta a diversas esferas y niveles de la actividad humana, modestamente se presenta esta obra como una aportación científica que, desde el MADOC y la Universidad de Granada, pretende indagar de una manera propositiva en algunas de las cuestiones más desafiantes de este complejo y atractivo reto que constituye la ciberseguridad.

Parte I

EL ESCENARIO GLOBAL DE SEGURIDAD ACTUAL

CARACTERES DE LOS CONFLICTOS ARMADOS CONTEMPORÁNEOS

Javier Roldán Barbero*

Palabras previas

En esta obra se habla abundante y cualificadamente de la ciberseguridad, un nuevo espacio sin fronteras, un reto mayúsculo ya del presente, y sobre todo del futuro. Los dominios de la (in)seguridad se van expandiendo material y espacialmente. En esta contribución nos situamos, sobre todo, en tiempo pasado y presente, orillando casi del todo los desafíos que el ciberespacio representa y poniendo el acento en otras modalidades de conflicto. El ciberespacio es, sin necesidad de recurrir a alienígenas, otro mundo…, que comparte, sin embargo, características con otros tipos de conflictos y de escenarios y con el panorama general de nuestro tiempo. A saber: el reto para los derechos humanos; las relaciones complicadas entre seguridad y libertad; el nuevo mapa geoestratégico con el ascenso de China; la mercantilización de las relaciones internacionales; el foso entre países prósperos y atrasados; la confusión entre lo verdadero y lo falso, entre lo bueno y lo malo y entre los héroes y los villanos; la interacción entre el ámbito público y el privado; la ineluctable integración europea; el uso dual de los avances científicos; la insoportable fugacidad y obsolescencia de nuestro tiempo y nuestros saberes, etc.

Una mirada comparativa hacia la historia

La violencia va ligada a la historia de la humanidad, se remonta a la noche de los tiempos. Se podría decir que es inherente a la naturaleza humana, si bien sigue la polémica viva sobre la

* Catedrático de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Granada (jroldanb@ugr.es).

condición primitiva del hombre entre *rousseaunianos* y *hobbesianos*. No es alentador pensar que la escuela llamada «realista» de las relaciones internacionales se caracterice por una visión más descarnada de los conflictos e intereses entre los países. Así las cosas, el adjetivo «humano» no debería tener las connotaciones virtuosas que reviste. Sin embargo, a pesar de lo que podría deducirse de los informativos (¡y del moderno cine de Hollywood!), se ha podido demostrar que la violencia ha ido declinando en nuestro mundo, al tiempo que ha cambiado nuestra condescendencia hacia ella y se ha revalorizado lo «humanitario» [1]. En términos más concretos, desgraciadamente, algunos países, como Costa de Marfil, han seguido el camino inverso: han pasado en los últimos años de la armonía interna a una alta convulsión social. ¡Habrá que esperar a que la tecnología del comportamiento humano se desarrolle sin deshumanizarnos como en «La naranja mecánica» o a que los científicos neuroéticos mejoren las bases cerebrales de la moralidad en el ser humano! Afortunadamente, los científicos también dicen que el altruismo forma parte de nuestra genética y de nuestra manera de ser feliz.

Las guerras han ido cambiando o segando la vida de las personas. Desde un punto de vista público, los conflictos armados han ido marcando la historia de las relaciones internacionales como *modo de arreglo de controversias*, y configurando su ordenamiento jurídico. «Son las guerras las que hacen los tratados», escribió Voltaire. No es extraño que algunos autores vean un precedente remoto del Derecho internacional en un tratado de paz alcanzado alrededor de 1285 a. de C. por Ramsés II de Egipto y el Rey de los hititas. Los estados de guerra y de paz, y su regulación jurídica, han llegado a dividir las enseñanzas y los tiempos del Derecho internacional, como ya hiciera en el siglo XVII Hugo Grocio, uno de los padres de esta disciplina, en su obra «Sobre la guerra y la paz». Un periodo de paz era caracterizado como un periodo de *entreguerras* (también ahora las treguas son utilizadas simplemente para rearmarse…). Es interesante indicar que la Paz de

1. Véase Pinker, S., *The Better Angels of Our Nature. Why Violence Has Declined*, Viking (2011).

Westfalia, de 1648, origen del sistema internacional de Estados, fue instituida para acrecentar la seguridad de unos y otros bajo el principio de la coexistencia pacífica entre las naciones. Es evidente que cualquier ordenamiento jurídico aspira a extirpar, o al menos a prevenir y aliviar, la violencia; ninguna sociedad, ningún ordenamiento jurídico, ni interno ni el internacional, ha logrado expulsar, sin embargo, la violencia armada. Los polemólogos sostienen que solo se han vivido 26 días sin guerra a partir de la Segunda Guerra Mundial.

Por otro lado, la guerra ha fermentado el mundo de la cultura para denostarla (el cuadro del «Guernica», convertido en un símbolo antibélico, lo mismo que películas como «Senderos de gloria», o piezas musicales como «A Mass for Peace»), aunque también para narrar algún episodio honorable (como retrata el cuadro de «La rendición de Breda»), o incluso para idealizarla bajos ropajes románticos, soslayando el componente de horror y terror que ineluctablemente encierra. Es verdad que la guerra puede, por sus convulsiones, por su daño indecible, crear buena literatura, aun basada en hechos reales. Es el caso de «La historia verdadera de la conquista de Nueva España», escrita por Bernal Díaz del Castillo en el siglo XVI, crónica considerada últimamente como una obra maestra de las letras. En el caso siniestro de México, el narcotráfico y la *guerra* contra este flagelo —que han provocado más de 50.000 víctimas mortales en los últimos años— ha sido fuente de buena literatura, buen cine y buena música.

Lo cierto es que la guerra ha sido un instrumento frecuente y lícito, durante siglos, de hacer política. En unas relaciones internacionales descentralizadas, basadas en una concepción absoluta de la soberanía del Estado, entendido como una *summa potestas*, era lógico que los países se enzarzaran a menudo en conflictos armados. Los esfuerzos doctrinales por encauzar la guerra fueron baldíos: la escuela española clásica de Derecho internacional (con Vitoria y Suárez a la cabeza) postuló que la guerra solo fuera librada cuando estuviese animada de una causa justa: lo que todavía, *mutatis mutandis*, se defiende desde diversos planos del mundo diplomático y académico. Emmanuel Kant, el filósofo alemán del siglo XVIII, por su parte, estaba persuadido de que las guerras se acallarían cuando se alcanzara

una paz perpetua que estaría basada en la generalización de los valores republicanos [2]. Esa paz perpetua ha figurado en tratados internacionales sin que su carácter formalmente vitalicio haya disipado las amenazas y las inquietudes [3]. Nada es irreversible en las relaciones políticas.

En los estudios e investigaciones militares ocupa un lugar destacado las «lecciones aprendidas»; es decir, las enseñanzas que se pueden extraer de los conflictos armados del pasado. Tiene, pues, interés echar la vista atrás y comparar la situación de antaño con la actual. Eso sí, sin contar batallitas…

Así hemos podido caracterizar a algunas tierras y a algunos pueblos como más pacíficos o más indómitos y convulsos. La historia de Afganistán es elocuente a este respecto, o la del Mediterráneo, por no hablar de la querencia en los Estados Unidos por las armas de fuego…; por otra parte, también tiene interés conocer que el pueblo iraní, más culto que la media regional, jamás ha emprendido guerras de agresión contra sus vecinos. La Historia sigue sobrevolando las relaciones internacionales contemporáneas en lo que a los conflictos se refiere: se sigue echando la historia a la cara. Se sigue exigiendo perdón por hechos y por personajes del pasado, y juzgando esos hechos y esos personajes, desproporcionadamente, desde la perspectiva del presente. Se sigue valorando, y detestando, a un país tercero, como Estados Unidos en buena parte del mundo árabe, por errores y abusos de otro tiempo, de otros gobiernos. Se tiende al maniqueísmo y a la simplificación, por ejemplo reduciendo la guerra española entre 1936-1939 a un mero conflicto entre fascistas y demócratas [4]. En

2. Sobre la evolución del tema de la paz en el campo doctrinal, véase De Lucas, «La paz imposible. De Erasmo a Kelsen», en Martínez de Pisón, J.M. y Urrea, M., *Seguridad internacional y guerra preventiva. Análisis de los nuevos discursos sobre la guerra*, Perla Ediciones (2008), págs. 31-58.

3. Así, en la Gaceta Oficial de 5.06.1860 se publicó el Tratado de Paz y Amistad, de ese mismo año, entre España y Marruecos. En su artículo 1 se enuncia que «Habrá perpetua paz y buena amistad entre S.M. la Reina de las Españas y S.M. el Rey de Marruecos y entre sus súbditos».

4. Las divergencias doctrinales se han acentuado precisamente en los últimos años. A la aparición de un diccionario promovido por la Academia española de la Historia, con una visión más benévola hacia el bando sublevado y el cau-

realidad, la mayoría de los soldados que han batallado en esta y otras guerras del pasado y del presente no han sabido muy bien por qué mataban ni querían hacerlo, ni tenían una ideología ni alineamiento muy precisos. Las diferentes maneras de entender un conflicto armado siguen provocando desavenencias en un mismo país (el ejemplo de España con su guerra civil es ilustrativo) o en las relaciones entre países (piénsese en las islas Malvinas, bajo soberanía británica y reivindicadas por Argentina). Disputas del presente, sobre todo territoriales, se remontan en sus orígenes y en sus fundamentos varios siglos atrás y siguen estando orientadas por sucesos y tratados de otro tiempo (podríamos referir el conflicto de Gibraltar y el Tratado de Utrecht, ya tricentenario). Algunos gobiernos en apuros siguen inflamando a sus poblaciones y curándose en salud con los problemas del presente blandiendo lances armados de antaño (la conquista española de América es aún argumento político actual). Bien es verdad que en otras ocasiones el mismo recuerdo de la guerra sirve para pacificar y encarrilar de forma armoniosa la situación actual: nuestra guerra civil y nuestra Transición podrían ilustrar esta afirmación, de la misma forma que la maldición de las tres guerras, en menos de un siglo, libradas por Francia y Alemania sirvieron para fundamentar y legitimar la integración europea. El problema ahora de la Unión Europea, entre otros, es que las nuevas generaciones desconocen el profundo valor pacificador y político que tuvieron las primitivas Comunidades Europeas, concebidas como instrumento de paz, y no solo como mecanismo de crecimiento económico. De ahí que el Premio Nobel de la Paz que le ha sido concedido a la Unión en 2012 sea muy justo. El nacionalismo exacerbado arrastra los peores males a la humanidad. «Amo demasiado a mi país como

---

dillo Franco, se ha replicado, en especial, con la obra editada por Viñas, Ángel, *En el combate por la historia. La República, la Guerra Civil, el franquismo*, Barcelona (2012). Cabe pensar ahora, y desear para el futuro, que los acontecimientos desautoricen los versos de Ángel González de que la historia de España se parece a la morcilla en que ambas están hechas de sangre y ambas se repiten. También los versos de Jaime Gil de Biedma no responden hoy, afortunadamente, a la realidad, cuando señalaba que de todas las historias tristes de la Historia la más triste es la de España porque siempre acaba mal.

para ser nacionalista», escribió Albert Camus. De ahí que la cooperación y el entendimiento internacionales sean siempre una buena fórmula de reparación de las heridas del pasado. La negociación entre antiguos enemigos, afortunadamente, nunca debe ser descartada. Se dice que la paz solo se firma entre rivales. Otra cosa es el precio político que se debe pagar por la reconciliación. La historia nos enseña que líderes políticos han evolucionado, y han sido caracterizados, alternativamente, como hombres de paz o de guerra (Kissinger o Arafat merecieron el Premio Nobel de la Paz, también Barack Obama[5]…).

Naturalmente, las cosas han cambiado sustancialmente, también en la naturaleza y las modalidades de los conflictos bélicos. Antes se exigía una declaración formal de guerra; ahora el término se rehúye, de manera que se puede polemizar sobre qué situaciones merecen este calificativo y cuál es la duración real de la contienda. Otrora algunas guerras se extendían décadas en el tiempo: la guerra de los 100 años, la de los 30 años. Actualmente, su extensión puede ser discutida: ¿13 años se puede decir que durará el conflicto armado en Afganistán, uno de los más largos de nuestra época? Además, la situación formalmente post-bélica —y el mismo anuncio y ejecución del repliegue— pueden ser tanto o más violentos que la situación precedente. Por eso se habla, junto a un *ius ad bellum* y a un *ius in bello*, de un *ius post-bellum*. Las heridas de la guerra tardan mucho en cicatrizar, y como señalé, sus secuelas en el terreno político perduran mucho tiempo. La reconciliación será más difícil cuanto más virulenta y prolongada haya sido la contienda, cuantos más agravios y sufrimiento hayan sido causados. El ejemplo de Irak, ya en nuestro siglo XXI, salta enseguida a la memoria, y pone de relieve la importancia de otra rama

5. Precisamente, es interesante reflexionar sobre el margen de pacifismo que el *establishment* estadounidense permite a su Presidente, el cual tiene licencia para autorizar un asesinato en el extranjero y se ve condicionado por una opinión pública que puede acusarlo de «paloma» por ser demasiado condescendiente, tímido en la escena internacional. Sobre estas cuestiones, y en especial sobre la concentración excesiva de poderes en la Presidencia en el ámbito militar, trata el libro de Wills, G., *Bomb Power. The Modern Presidency and the National Security State* (2010).

jurídica: el derecho de la ocupación. En este caso se comprueba que la violencia se hace más desordenada, menos formalizada. Se habla de guerras asimétricas, en las que el combatiente enemigo sin Estado no está identificado. Claro que la guerra de guerrillas, que tanto mal hace a los Estados hoy en día y que favorece a la parte militarmente más endeble, no es un invento de ayer: ya el pueblo español empleó esta táctica en la guerra de 1808… Siguen, por otra parte, manteniéndose estados formales de guerra, aunque, como antaño, no siempre se trata ininterrumpidamente, por suerte, de guerras calientes. Añadamos algo más a este propósito: en ocasiones, la victoria de un bando radical desencadena una espiral de represión entre la población, de ajustes de cuentas, que supera en número de muertos el habido durante la contienda propiamente militar. La dictadura, civil o militar, puede ser peor que la contienda abierta. El balance de un conflicto también es desolador cuando se comprueba la cantidad de dolor y tristeza que ha causado, para nada (podríamos hablar de ETA).

Es indudable que nuestro volumen de información y de opinión sobre un conflicto armado de nuestros días es mucho mayor que el de otro tiempo. A tal fin colaboran evidentemente las nuevas tecnologías. Sin embargo, sigue imperando la frase de que en un estado de guerra la primera víctima es la verdad. Junto al teatro de las hostilidades, las partes contendientes e involucradas desarrollan una guerra de propaganda, también importante para legitimar en términos políticos y jurídicos su posición y ganar confianza restándosela al enemigo. No siempre la batalla política y la militar tienen al mismo ganador, aunque con razón se diga que la historia la escribe el vencedor. El vencedor, como nuevo gobierno de facto del país, termina normalmente entablando relaciones diplomáticas con casi todos los países, aun con encarnizados adversarios durante las hostilidades. En ocasiones se llega a ignorar quién es el responsable, y en qué medida, de un determinado episodio sanguinario (quizá cometido por la misma parte damnificada para desacreditar ante la comunidad internacional al adversario). Los servicios secretos no siempre pueden acceder en buenas condiciones a la información. Los medios de comunicación son también víctimas, a veces mortales, como observadores y relatores privilegiados de lo que está ocu-

rriendo; en ocasiones, su propio alineamiento ideológico o hasta su manipulación de los hechos (¡no dejes que la realidad empañe un buen reportaje!) puede contribuir a la confusión, y no a la clarificación, de los acontecimientos. Tan malo es el exceso como la escasez de información. Sin embargo, las vivencias y memorias de los grandes reporteros de guerra nos ofrecen un testimonio vívido sobre los límites de la maldad y crueldad humana (o también de su solidaridad) [6]. El propio Internet, que puede condicionar ennobleciendo o envileciendo un conflicto, puede embrollar más el estado de cosas. No olvidemos tampoco en este orden de ideas la ocupación de Irak ocurrida en 2003 sobre la base de argumentos (como la tenencia de armas de destrucción masiva o la instigación del terrorismo internacional) que se revelaron falsos. Desgraciadamente, también ha resultado falaz la opinión de que la violencia cesaría una vez se hubieran retirado las fuerzas internacionales del territorio. Por todo lo cual se entiende que ante los conflictos armados un medio necesario de arreglo de la controversia sea la investigación, la determinación de los hechos: no siempre está claro quién es el agresor y quién el agredido, y en qué proporción, ni si esas posiciones se mantienen a lo largo de las operaciones bélicas. A veces, como sabemos, ni el mismo estado de guerra queda del todo resuelto: hay demasiadas guerras larvadas, no siempre de alta intensidad. Pero su resonancia internacional depende también del interés e intereses que susciten en la opinión pública internacional y en la diplomacia. No todas las muertes encierran el mismo tratamiento informativo, y a veces la carnicería se multiplica precisamente para atraer la atención del «ciudadano global» o para obligar a la negociación en situación de inferioridad a la otra parte. De algunos conflictos nos olvidamos, los damos por resueltos o encarrilados, y no es así: simplemente, no nos enteramos.

6. Puede verse el testimonio de la reportera de *Le Nouvel Observateur*, Daniel, Sara, *Guerres intimes*, Flammarion, (2012). También la historiografia militar ha avanzado en las últimas décadas hacia una narración más humanista de las batallas. Un pionero en esta tendencia fue (ya en su primera obra) Keegan, John, *El rostro de la batalla* (1960) y editada por primera vez en español en 1990 por el Servicio de Publicaciones del Ejército de Tierra.

Tras haber expuesto estas ideas preliminares, veamos con más detalle algunas otras características que también presiden los conflictos armados en nuestro tiempo. Una de esas características es la mayor regulación y supervisión jurídica, aun con sus fallas y contradicciones, incluso con sus intentos de involución en la abolición del *ius ad bellum*, como pretende la teoría de la guerra preventiva en legítima defensa (la aplicación de la autodefensa en el ciberespacio merece más comentarios) [7]. Hasta las ramas jurídico-internacionales centenarias, como el derecho de la neutralidad o como el *ius in bello*, han de adaptarse a los nuevos tiempos, a las nuevas modalidades de conflicto armado [8]. En general, todo fenómeno jurídico se mide por su capacidad para contener la violencia y está llamado a ser un instrumento formidable para alcanzar y preservar la paz, y a este respecto, parafraseando el título de una buena película española, muchas veces sí hay paz para los malvados. En todo caso, la vertiente propiamente jurídica del uso de la fuerza armada fue objeto de un estudio previo de este autor, por lo que aquí prescindimos de su análisis separado [9].

7. Véase Ramón Chornet, C., «Sobre la legitimidad internacional de las guerras preventivas», en Martínez de Pisón, J. M. y Urrea, M., *Seguridad internacional y guerra preventiva. Análisis de los nuevos discursos sobre la guerra*, Perla Ediciones (2008), págs. 201-228; también en relación con este concepto, Gutiérrez Espada, C., «Los conceptos de guerra preventiva y de legítima defensa preventiva a la luz de la jurisprudencia internacional contemporánea», en Martínez de Pisón, J. M. y Urrea, M., *Seguridad internacional y guerra preventiva. Análisis de los nuevos discursos sobre la guerra*, Perla Ediciones (2008), págs. 249-282.

8. Puede consultarse Matheson, M.J. y Montaz, D., «Les règles et institutions du droit international humanitaire à l'épreuve des conflits armés récents», *Académie de Droit International de La Haye* (2010).

9. Véase Roldán Barbero, J., «El nuevo panorama de la paz y la seguridad internacionales y su reglamentación jurídica», en Liñán Nogueras, D.J. y Roldán Barbero, J. (eds.), *El estatuto jurídico de las Fuerzas Armadas españolas en el exterior*, Plaza y Valdés (2008), págs. 13-38. Véase también a este propósito García Rico, E. M., «Los conflictos armados del siglo XXI: ¿nuevos conflictos, viejas normas?», en Martín y Pérez de Nanclares, J. (coord.), *Estados y organizaciones internacionales ante las nuevas crisis globales*, Iustel (2010), págs. 511-523; asimismo de interés Gordo García, F., «Perfil y tipología de los conflictos armados actuales», en Robles Carrillo, M., (coord.), *Género, conflictos armados y seguridad. La asesoría de género en operaciones*, Universidad de Granada (2012), págs. 3-50.

Las características dominantes en los conflictos armados actuales

La mayor naturaleza y repercusión internacional del conflicto

A pesar de este enunciado, una seña de identidad en este ámbito de nuestro tiempo es que cada vez son más raras las guerras originaria y formalmente interestatales. Por el contrario, menudean los conflictos originaria y formalmente internos, aunque bien es verdad que, más pronto que tarde, cualquiera de estos conflictos, digamos fratricidas, se proyecta y repercute en el escenario internacional, especialmente en la estabilidad y neutralidad de los vecinos con problemas de control de fronteras, flujo masivo de refugiados, declive económico, etc. Ya nuestra guerra civil fue entendida como un ensayo de la segunda guerra mundial. Claro, cuando hablamos de violencia interna no se puede soslayar la situación de criminalidad estructural que sufren muchos países. Es el caso de América Central, donde Honduras y El Salvador presentan cifras de muertes violentas superiores a las del actual Afganistán, y la inmensa mayoría de los delitos no se resuelven. En la ciudad de Caracas entre 40 y 70 personas mueren de esta forma cada fin de semana. Como se ve, la inseguridad ciudadana puede ser más letal que un conflicto propiamente armado, aunque algunos terroristas religiosos comienzan a proceder del campo de la pequeña delincuencia común: es éste solo una de las conexiones existentes entre la delincuencia política y la delincuencia común (la guerrilla colombiana de las FARC, por ejemplo, ha acabado mezclando su lucha política con el negocio del narcotráfico). En nuestro país, los estudios del Centro de Investigaciones Sociológicas (CIS) revelan que la inseguridad ciudadana es una preocupación importante de los españoles mientras que la seguridad internacional, como tal, no figura en este listado [10]. Es verdad que, como decimos, la seguridad interna y la internacional tienden

10. Véase por ejemplo el barómetro del CIS hecho público el 7 de marzo de 2012. En él figura la «inseguridad ciudadana» como sexto problema en España, mientras que el ámbito propiamente internacional de la seguridad no aparece entre las quince principales preocupaciones.

a entremezclarse, de la misma forma que lo hacen la seguridad pública y la privada. Así, en España, el terrorismo de ETA ha tenido conexiones y combates exteriores, en tanto que el terrorismo *yihadista* reviste connotaciones internas. No siempre está clara la distinción entre el enemigo interno y el externo (a veces, se busca un enemigo y un conflicto externos para opacar los problemas internos). En general, la delincuencia, sobre todo la organizada, se ha convertido en una cuestión reglada en el plano internacional [11].

Así pues, una gran parte de los conflictos que pueblan las noticias obedecen al desfallecimiento de un solo Estado, de un derecho interno, más que del Derecho internacional propiamente. Se genera de este modo la categoría del Estado «fallido» o «fracasado». Las instituciones nacionales son incapaces de mantener el orden, incluso son incapaces de alcanzar al conjunto del territorio estatal. En ocasiones, ante la proliferación de poderes, se ignora quién es el verdadero interlocutor, y con qué poderes y con qué fiabilidad, para iniciar un proceso de paz. La fortaleza del Estado se convierte, por consiguiente, en un valor indispensable para la convivencia internacional, a la vez que la incapacidad para la concordia interna se erige en factor que incapacita el progreso y la modernización del propio país. En el caso reciente de Sudán, la escisión y creación de un nuevo Estado (Sudán del Sur) no ha hecho sino reproducir a nivel ya interestatal la conflictividad que existía anteriormente en el interior de las fronteras del Sudán unificado. Se entiende, pues, que la regulación del derecho de los conflictos armados se haya extendido y singularizado para los conflictos internos (Protocolo II adicional a los convenios de Ginebra de 1949, relativo a la protección de las víctimas de los conflictos armados no internacionales, de 1977) [12]. Ante este estado de cosas, no se puede decir siempre, ni apropiadamente, que se ha muerto por la propia patria.

11. Véase, a este respecto, el Acuerdo de cooperación en materia de lucha contra la delincuencia entre el Reino de España y la República de la Costa de Marfil, publicado en el BOE de 13.09.2012.

12. Cfr. Mangas Martín, A., *Conflictos armados internos y Derecho internacional humanitario*, Universidad de Salamanca (1992).

Nos encontramos ante una nueva manifestación de la íntima relación entre lo interno y lo internacional, ante una nueva vertiente de la interdependencia entre las naciones. Tomemos el ejemplo reciente de Mali: un golpe de Estado militar en 2012 ha incentivado el movimiento secesionista de los tuaregs al norte del país y, posteriormente, la toma de esta parte del territorio por salafistas que pretenden imponer la *sharía* en esta región. Pues bien, este estado de cosas resulta inaceptable para la comunidad internacional, ya que el poder integrista, más allá del régimen ominoso impuesto en su territorio y a sus habitantes, amenaza con convertirse, no lejos de las fronteras europeas, en un foco de exportación del terrorismo fundamentalista que amenace, por lo demás, la labor de los cooperantes extranjeros en la zona. Como también se ha observado en el caso de Haití, el problema de seguridad interna, de orden público en un país deviene en un problema para la paz y la seguridad internacionales. Otras veces, la misma legislación interna de un país (como sucede con la permisividad con la venta y tenencia de armas de fuego en los Estados Unidos y respecto al consumo de estupefacientes) fomenta la violencia en el país contiguo (como sucede en México con la guerra del narcotráfico).

Ante los desafíos exteriores que afectan a la seguridad y libertad de un país, se comprende que en un país como España sus fuerzas armadas hayan ido adquiriendo en los últimos 30 años un marcado perfil internacional, en especial en lo que se refiere a sus misiones de paz exteriores, que han diversificado y prestigiado la política internacional del Estado [13]. Formalmente, este espíritu internacio-

13. Las manifestaciones de esa actividad internacional se multiplican. Por citar ejemplos hechos públicos en 2012, podemos citar el Tratado hecho por España con Francia, Italia, Países Bajos y Portugal por el que se crea la Fuerza de Gendarmería Europea (BOE de 1.06.2012). También el Memorando de Entendimiento suscrito por nuestro Ministerio de Defensa con sus homólogos de otros países en relación con la forma de onda de banda ancha para conexión en red en coalición. BOE de 27.04.2012. Véase al respecto Marrero Rocha, I., *La participación de las Fuerzas Armadas españolas en misiones de paz*, Plaza & Valdés, (2007). También Roldán Barbero, J., «La política española de seguridad y defensa. La vertiente exterior de las Fuerzas Armadas», en Roldán Barbero, J., *La nueva política de seguridad y defensa de la Unión Europea*, Universidad de Granada, (2012), págs. 187-221.

nalista queda muy atenuado en la nueva Directiva sobre la Defensa Nacional 1/2012, aunque es de prever y esperar que ese espíritu más doméstico no se traslade apenas a la práctica [14]. En cualquier caso, en razón de las amenazas de uno y otro signo, normalmente interconectadas y transversales, se entiende la recién creación, en el marco de la Presidencia del Gobierno, de un Departamento de Seguridad Nacional [15]. En términos más generales, el círculo de potencias que se ven interesadas o concernidas de alguna forma por un conflicto armado, aun los de naturaleza inicial y fundamentalmente interna, se ha ido ampliando: piénsese, como botón de muestra, en los países de tránsito obligado para el abastecimiento de una operación de mantenimiento de la paz [16]. No solo se trata, como decía, de los vecinos, que ven afectados sus intereses, a menudo alineándose con alguna de las facciones en lucha. Asimismo, ante conflictos de naturaleza estratégica, terceras potencias se implican en un sentido o en otro, a veces cambiando su propio

14. En efecto, la nueva Directiva sobre la Defensa, la 1/2012, firmada el 1 de agosto, ha sido caracterizada como más endogámica, más atenta a un planteamiento interno de la seguridad, a las amenazas exclusivas sobre España, y no tanto de las amenazas compartidas, lo que se ha interpretado como una referencia velada a las ciudades españolas del Norte de África. De hecho, la situación de amenaza de Ceuta y Melilla ha sido objeto de algún pronunciamiento judicial, si bien finalmente los procesados fueron absueltos del delito de integración en organización terrorista. Véase la Sentencia de la Audiencia Nacional (Sección Cuarta) de 25.04.2012. En esta resolución se dice que «no consta indubitadamente acreditado que ninguno de ellos pretendiera atentar contra intereses o plazas españolas o que fueran los responsables o instigadores» de las acciones que les imputa la Fiscalía. En este sentido, es evidente, y criticable, como digo, la «desinternacionalización» que este documento estratégico conlleva, postergando el enfoque multilateral, aunque probablemente tal cosa no se va a traducir a la práctica. La crítica desde la oposición socialista está condensada en López Garrido, D., «Defensa nacional: regreso al pasado», *El País*, 10.08.2012.

15. Real Decreto 1119/2012, de 20 de julio. BOE de 23.07.2012.

16. Véase el Acuerdo entre el Reino de España y el gobierno de la República de Kazajstán sobre el tránsito de equipos y personal militares a través del territorio de la República de Kazajstán con motivo de la participación del Reino de España en los esfuerzos internacionales para la estabilización y reconstrucción de la República Islámica de Afganistán, hecho en Astana en julio de 2009 y publicado, tardíamente, en el BOE de 23.06.2012.

criterio a medida que la guerra se va desenvolviendo. En el trágico caso de Siria apreciamos el conflicto regional con Irán a favor del déspota el Asad y con Arabia Saudí y, en general, las naciones de mayoría suní, implicadas a favor de la insurgencia. Más aún, las grandes potencias también se posicionan: Rusia y China, a favor del sátrapa, y las potencias occidentales, más favorables al bando rebelde. La implicación exterior ora resuelve, ora azuza el conflicto bélico interior. La complejidad del puzle se embrolla si tenemos en cuenta las fracturas que se producen en ambos bandos; así entre los rebeldes hay discordancias entre los sirios del interior y los del exilio. No faltan tampoco intereses puramente personales en la zona con la presencia de francotiradores o de integristas procedentes de otros países. Sobre este orden de ideas, la condena histórica dictada por el Tribunal Especial para Sierra Leona contra el exdictador de Liberia Charles Taylor, que se lucró de los «diamantes de sangre», corrobora la dilución de la línea divisoria entre lo privado y lo público, lo interno y lo externo en los conflictos armados [17].

Tras el fin de la guerra fría, marcada por la bipolaridad (y por la extensión por parte de las superpotencias de sus redes de influencia en otras regiones), emergió Estados Unidos como única potencia, como la «nación indispensable», cuyos intereses cubrían todo el planeta, y que impondría una *pax americana*. En especial, Oriente Próximo es una región donde se concitan altos intereses globales. Estados Unidos ha hecho de su protección a Israel una misión moral e histórica, y los intereses del Estado hebreo, lógicamente, se proyectan a procesos tales como la revolución en Egipto o el programa nuclear en Irán [18]. Sin embargo, una cierta decadencia advertida en Estados Unidos, entendido en un

17. Sentencia de 27.04.2012. Esta decisión es la primera que dicta la justicia internacional contra un exjefe de Estado. El Tribunal declara probado que Taylor instigó las matanzas perpetradas entre 1991 y 2002 por el Frente Revolucionario Unido de Sierra Leona, si bien lo absuelve de la responsabilidad directa de los hechos.

18. Téngase presente, por ejemplo, que Estados Unidos viene destinando cada año 1.300 millones de dólares a Egipto en concepto de ayuda militar, y que una de las condiciones de ese envío es salvaguardar la coexistencia pacífica con Israel.

famoso libro como «Marte» frente a la Europa caracterizada como «Venus» [19], está reorganizando el mapa geoestratégico global, más enfocado ahora hacia el Pacífico que hacia el Atlántico, con las consecuencias correspondientes para la seguridad y defensa europeas. Téngase en cuenta que en 2011 por primera vez Asia superó a Europa en gasto armamentístico y que los cinco principales importadores de armas son de aquel continente [20]. China, en concreto, anuncia que aumentará su gasto en Defensa en 2012 un 11.2 %, según las cifras oficiales, que quizá se quedan cortas. Esta militarización, aun bajo el eslogan oficial del país de «ascenso pacífico», está reorientando la estrategia en seguridad a escala mundial (también América Latina experimenta un incremento en la partida militar). Hay que admitir que de la ocupación de Irak y de la inacción armada ante Corea del Norte o Irán se ha derivado una triste enseñanza: la tenencia de armamento, especialmente de destrucción masiva, es una vía eficaz para disuadir, y no sufrir, la intervención militar exterior. Por otra parte, determinados conflictos terminan exportando la violencia más allá, como ha pasado con el conflicto en Libia, que ha generado mercenarios armados en Malí, por ejemplo.

Por otra parte, el terrorismo de raíz islamista ha emergido como una amenaza firme para la estabilidad y libertad mundiales. En los últimos tiempos se han desarticulado varios complós que, de haberse llevado a término, habrían cambiado muchas cosas en la visión de nuestro tiempo y nuestro mundo (como ya pasó con los atentados contra las Torres Gemelas de Nueva York). La «geografía» de este terrorismo ofrece una paradoja a menudo desapercibida: son los países y las personas musulmanes las principales víctimas de esta violencia integrista, a menudo

19. Véase Kagan, R., *Of Paradise and Power: America and Europe in the New World Order*, New York (2003).

20. Datos del Anuario correspondiente a 2011 del Instituto Internacional de Estudios para la Paz (SIPRI) radicado en Estocolmo. En efecto, en este volumen se recoge que los principales importadores de armas del mundo son India, Corea del Sur, Pakistán, China y Singapur. En el capítulo de exportadores sobresalen Estados Unidos, Rusia, Alemania, Francia y Reino Unido.

envuelta en disputas sectarias [21]. Se producen, en este contexto, matanzas entre compatriotas y correligionarios que no responden básicamente a un conflicto interno. No toda la violencia de raíz islamista responde a un «conflicto de civilizaciones», según la famosa fórmula acuñada en 1993 por Samuel Huntington. La violencia en Afganistán y Pakistán están interconectadas, de modo que no se sabe si este último país resulta más amenazante para la seguridad internacional que Afganistán, donde se han desplegado las misiones internacionales [22].

La mundialización de los asuntos relativos a la paz y seguridad, aun los de carácter originariamente nacional, ha multiplicado en los últimos 25 años la actividad, aunque no siempre la eficacia, del Consejo de Seguridad de Naciones Unidas, garante primordial del mantenimiento de la paz y seguridad *internacionales*. Sin embargo, también para este órgano hay guerras de primera y segunda categoría, vívidas y olvidadas, así como un doble rasero a la hora de abordarlas [23]. También hay que consignar que el marco universal tiende a delegar o a servirse del marco regional, buscando una mayor implicación de los actores más concernidos [24]. Este dato explica el mayor protagonismo adquirido en las últimas revoluciones por organismos como el Consejo de Cooperación del Golfo, la Liga Árabe o la Comunidad Económica de África Occidental. Al mismo tiempo, esta circunstancia es causa y consecuencia, a la vez, de la emergencia de nuevos poderes estratégicos como Turquía o Arabia Saudí ante el declive de los poderes occidentales. Lo cierto es que la

21. Puede consultarse Reinares, F., «Geografía mundial del terrorismo», *Análisis del Real Instituto Elcano*, núm. 95 (2012), págs. 4-9.

22. Cfr. Pozo Serrano, P., *La guerra de Af-Pakistán y el uso de la fuerza en las relaciones internacionales*, Pamplona (2011).

23. Es significativo que, ante la inacción del Consejo de Seguridad ante el conflicto sirio (fundamentalmente por el veto chino-ruso), la propia Asamblea General de la ONU ha deplorado este estado de cosas en su resolución A/66/L57, aprobada en 3 de agosto de 2012.

24. Sobre esta cuestión, véase el curso de Boisson de Chazournes, L., «Les relations entre organisations régionales et organisations universelles», *Recueils des Cours de l'Académie de Droit International de La Haye*, núm. 347 (2010), págs. 238-347.

comunidad internacional es una parte involucrada, junto a los contendientes, en los conflictos armados que proliferan en el mundo. En conflictos exteriores, como el de Siria, se siguen, como señalé, atisbando coletazos de la guerra fría entre Occidente y Rusia. También se aprecian en el despliegue del escudo antimisiles, cuyo componente naval se situará en Rota. En esta iniciativa Rusia ve una maniobra contra su sistema de disuasión nuclear, en tanto que Estados Unidos asegura que el escudo está pensado para misiles provenientes de Irán o Corea del Norte: un ejemplo, por lo demás, de las dudas que se ciernen a menudo sobre el tipo y el origen del ataque contra el cual nos estamos preparando. En cualquier caso, lo que sí resulta meridianamente claro es que gran parte de los conflictos armados que sacuden a un Estado, y por extensión el panorama internacional, no pueden solucionarse sin una intervención externa, a veces sin la implicación de un determinado país. En todo caso, se ha instalado ya indiscutiblemente un derecho de injerencia, de la misma forma que antes se entendía que la violencia en el interior del hogar formaba parte del ámbito reservado, y ahora por fortuna se ha convertido en un problema de interés y regulación públicos. La magnitud y la naturaleza de esta injerencia es el objeto de grandes discusiones que veremos más adelante al referirnos a la tutela de los derechos fundamentales.

La mayor privatización de los conflictos

Es el signo de los tiempos: los problemas financieros de los Estados junto a la mayor implicación, para lo bueno y lo malo, de los particulares en los asuntos internacionales han provocado, también en el terreno de la violencia, una mayor privatización. En este campo, específicamente, la multiplicación de conflictos dentro de los Estados y no entre ellos acentúa la implicación de la ciudadanía en los disturbios. De resultas de ello, se difumina la clásica distinción del derecho humanitario bélico entre población civil y población militar, siendo siempre muy elevado el balance de víctimas civiles, muchas veces utilizadas como escudo humano.

Este fenómeno se aprecia en los dos lados de la violencia:

En primer lugar, desde el punto de vista de las fuerzas del orden, los ejércitos, uno de los vectores regalianos de los Esta-

dos [25], experimentan una cierta delegación en empresas particulares, de manera que se crean agencias de seguridad privadas paralelas a las gubernamentales, algunos de cuyos servicios son subcontratados, al tiempo que aumenta la colaboración entre la seguridad pública y privada, como se ha puesto de manifiesto en la lucha librada por España contra la piratería en el Golfo de Aden. Así asistimos a fuerzas paramilitares cuyo estatuto jurídico no está bien definido y que resultan inquietantes para los derechos y libertades de los ciudadanos [26]. Recuérdense los escándalos protagonizados por la empresa norteamericana llamada por entonces *Blackwater* durante la ocupación de Irak.

En el lado contrario, desde el punto de vista de la comisión de actos armados, es un lugar común en nuestros días advertir la proliferación de guerras asimétricas ante la eclosión de grupos armados de particulares con una gran capacidad letal. El enemigo para Occidente ha cambiado, pues, de rostro desde los tiempos de la guerra fría (un bando identificado, la Unión Soviética y sus satélites) hasta los actuales, fundamentalmente el integrismo islámico. Este estado de cosas se ha acentuado en los últimos tiempos con la aparición de «lobos solitarios», individuos que actúan aisladamente, aunque con colaboración y difusión en las redes sociales, causando el mal en cualquier parte en nombre del Islam y sustentados en conflictos internacionales tales como el contencioso israelo-árabe o la presencia de tropas occidentales en Afganistán. Ya se sabe que la lucha contra el pueblo judío (y la de Israel contra sus enemigos) puede tener cualquier escenario, mejor cuanto más impacto informativo mundial tenga. El análisis

25. Está extendida en todos los ordenamientos jurídicos la atribución de la Defensa exclusivamente a la administración general del Estado, tal como sucede en nuestro país. La sensibilidad de la materia también hace que todos los países blinden el sector frente a la inversión extranjera, de modo que la Defensa queda sustraída o limitada a las reglas del libre mercado.

26. Véase Torroja Mateu, H., (dir.) y Guéll Peris, S. (coord.), *La privatización del uso de la fuerza armada. Política y Derecho ante el fenómeno de las «empresas militares y de seguridad privadas»*, Bosch (2009). También Espaliú Berdud, C., *El estatuto jurídico de los mercenarios y de las compañías militares privadas en el Derecho internacion*al, Thomson-Aranzadi (2007).

de la estructura de estos grupos, a veces coligados, a veces independientes, es objeto de estudio para los analistas del fenómeno, muy demandados a partir del «11-S». No es raro, empero, que estos grupos tengan la financiación e instigación de algún Estado (así ocurre con la poderosa guerrilla prosiria Hezbolá) ni que la misma *yihad* se apropie de territorios en los que pasa a convertirse en la autoridad pública que practica la *sharía*, al menos temporalmente, como ha sucedido en Somalia o en el norte de Mali. La lucha contra este flagelo por parte de los Gobiernos desencadena un debate intenso sobre las relaciones entre la seguridad y la libertad. El Consejo de Seguridad de Naciones Unidas establece sanciones a una lista de particulares, sanciones cuya legalidad en el marco de la protección de los derechos humanos, ha sido sometida en varias ocasiones al escrutinio del Tribunal de Justicia de la Unión Europea [27]. La tristísima experiencia del 11-M en Madrid en 2004 nos enseñó que la capacidad de infligir horror y terror por una suma pequeña de dinero (en torno a los 50.000 euros) es muy grande.

Por otra parte, el comercio internacional de armas, que capea bien la crisis económica, experimenta un desorden que escapa a las manos de los Estados. El panorama de proveedores y compradores de armas se ha hecho más complejo, sobresaliendo los clientes y suministradores privados, cosa que no deja de preocupar a los mismos Gobiernos. En este contexto de creciente competencia internacional hay que ubicar un Real Decreto-Ley aprobado en España a fin de procurar el contrato de venta de armas «Gobierno a Gobierno», de manera que el Gobierno español ejerza de vigía garante de la operación realizada por una empresa española del sector con un Gobierno extranjero [28] (ha sido el caso de la venta

27. Véase Hinojosa Martínez, L. M., Pérez Bernárdez, C., «El derecho a la tutela judicial efectiva en el Derecho europeo y las sanciones contra Al-Qaeda», en *Estudios de Derecho internacional y europeo en homenaje al prof. Manuel Pérez González*, Tomo II, (2012), págs. 1569-1603. Véase Santos Vara, J., «The Consequences of Kadi: Where the Divergence of Opinion between EU and International Lawyers Lies?», *European Law Journal*, (2010).

28. Real Decreto-Ley 19/2012, de 25 de mayo, de medidas urgentes de liberalización del comercio y de determinados servicios. BOE de 26.05.2012.

de 250 carros de combate a Arabia Saudí por parte de la empresa General Dynamics Santa Bárbara). El intento de embridar este comercio en lo que se refiere a las armas ligeras se saldó con un fracaso en la Conferencia internacional convocada a tal efecto en el verano de 2012. En otros capítulos, como el nuclear, también su posesión por particulares fue objeto específicamente de una conferencia internacional en marzo de 2012 en Corea del Sur por parte de 53 Estados, temerosos del contrabando y el terrorismo nucleares. En la declaración final se insiste en la responsabilidad de los Estados de mantener la seguridad de todo el material nuclear a fin de impedir la adquisición de este material con fines criminales por actores no estatales. Sin embargo, se añade, tales medidas no impedirán el derecho de los Estados a desarrollar y utilizar la energía nuclear con fines pacíficos. Sigue habiendo partidarios de una doctrina MAD (destrucción mutua asegurada), consistente en la tolerancia hacia los programas nucleares con fines militares, en la idea de que esta estrategia serviría, como en los tiempos de la Guerra Fría, como instrumento disuasorio de futuros ataques…

Por tanto, el sector privado se ha convertido en un aliado en algunos aspectos del sector público en el negocio de la seguridad y de la violencia, pero en otros se ha convertido en una alternativa amenazante y descontrolada. Ya se sabe que las nuevas armas derivadas de las nuevas tecnologías, como los aviones no tripulados (*drones*) o los artefactos explosivos identificados (IED, por sus siglas en inglés) resultan ventajosas o peligrosas según en qué manos caigan y el uso que se haga de ellas, así como el prisma desde el que se vean las cosas. Muchos artefactos, además, están expuestos a un uso dual, civil y militar [29]. La diseminación de armas letales de distinta intensidad en manos de particulares supone un grave riesgo para la seguridad internacional, pero no conviene olvidar que algunos Estados representan un peligro de

29. Lógicamente, al margen del mercado internacional, lícito o ilícito, de armas existe una reglamentación jurídico-internacional a nivel público y transparente. Véase, como ejemplo, el Convenio para el reconocimiento recíproco de punzones de pruebas y armas de fuego portátiles. BOE de 28.05.2012.

mayor relieve. La historia en este sentido nos enseña que la mayor mortandad siempre es ocasionada por el sector público.

Una visión transversal de la paz y de la guerra

Cuestiones generales

Una forma tradicional de clasificar los enfoques doctrinales sobre la sociedad internacional ha sido distinguir los enfoques que enfatizan más la armonía entre las naciones y los que, por el contrario, enfatizan más el conflicto permanente. Más allá de este planteamiento académico y personal, ahora caminamos, afortunada y sensatamente, hacia una visión más holística, polifacética de la violencia internacional, hacia una paz estructural que esté entroncada con los demás bienes públicos globales, con el resto de los principios rectores del sistema internacional, de forma que se ejerza constantemente una diplomacia preventiva. Como tantas veces se ha dicho, la paz no es solo la ausencia de guerra, sino que ha de tener también una dimensión positiva. Siguiendo la terminología acuñada por Joseph Nye, en la diplomacia mundial gana terreno el *soft power*, la capacidad de seducción, frente al *hard power* (el empleo de la fuerza y de la coacción). No sorprende que entre los estudios de posgrado en nuestras universidades proliferen titulaciones centradas en distintos aspectos de la paz y de la guerra (en la polemología y en la irenología). El mundo sigue siendo, por muchos motivos, un lugar muy peligroso, aunque el riesgo —el valor de la vida humana— esté repartido muy desigualmente en términos geográficos, y el miedo sea algo, finalmente, muy íntimo y personal.

De resultas de esta visión integral, reflejada en la primera Estrategia española sobre el sector [30], a la seguridad en nuestros días se le añaden muchos adjetivos (y también algún prefijo: ciberseguridad, bioseguridad), y en más de un sentido. Así la «seguridad alimentaria» tiene una doble acepción en el mundo rico (referida

30. Sobre las perspectivas que presentaba esta Estrategia antes de su aprobación formal véase Arteaga, F., «Hoja de ruta para la Estrategia de Seguridad Nacional española», *Análisis del Real Instituto Elcano*, núm. 57, (2008), págs. 22-27. Un comentario de prensa tras su aprobación puede verse en Mangas Martín, A., «Estrategia española de seguridad», *El Mundo*, de 29.06.2011.

a la *calidad* de los alimentos) y en el mundo pobre (referida a la *cantidad* de los alimentos): la subida actual de los precios agrícolas (fruto de desastres naturales, como la sequía, pero también humanos, como la especulación) amenaza la vida de unos 1.000 millones de personas, según la ONG Intermón Oxfam. La rampante globalización hace que tengan un perfil internacional e interdependiente conceptos como la seguridad ecológica, la sanitaria (también hay enfermedades de ricos y enfermedades de pobres), o la energética. Vivimos tiempos de riesgos, de incertidumbres, de manera que podríamos hablar, en el sentido más amplio de la expresión, de una necesaria *seguridad social*. Evidentemente, esta seguridad polisémica no debe ser confundida con el indeseable dogmatismo que pontifica sobre presuntas verdades incontestables. Correlativamente, a la violencia se le añaden muy variados atributos: se ha llegado a hablar en nuestro país, con fundamento, de violencia urbanística… La concatenación de los miedos, riesgos y amenazas de distinta índole —podríamos hablar también de la llamada *bomba* demográfica [31]— puede formar un cóctel explosivo, aunque siempre es mejor pensar, por salud mental, como aquel autor que dijo que se había pasado la mitad de su vida preocupado por cosas que no han llegado a ocurrir… Sin embargo, este desentendimiento no es justificable en el poder público. A pesar de su aparente buena intención, se trata de una maldición decir: ¡ojalá tus hijos vivan tiempos interesantes…! Pensemos también que, en ocasiones, los mismos Gobiernos fabrican o alimentan esos miedos por intereses espurios.

Lo cierto es que el panorama internacional nos presenta amenazas, además de heterogéneas, de nueva planta, varias de ellas derivadas de los avances científicos, con el ciberespacio, claro está, en un primer plano [32]. Ya se sabe que el desarrollo científico

31. El factor demográfico tiene elementos inquietantes ciertamente, aunque también alguno tranquilizador, como que una población de edad media más avanzada, se supone, no tendrá los ardores belicistas y transformadores que se atribuyen a la juventud.

32. Un panorama de algunas de estas amenazas es trazado en el número monográfico de la *Revista Ejército de Tierra Español* dedicado a los «Retos, riesgos y amenazas al inicio del siglo XXI», núm. 837 (2010). Otro tipo de análisis se

puede ser utilizado para lo mejor y para lo peor en materia de seguridad, y que por tanto entraña riesgos y oportunidades en este campo. Otros temas que penetran en la paz y seguridad internacionales son, en cambio, tradicionales. Estoy pensando ahora en la religión, concebida para proporcionar confort, esperanza y *paz interior* (y también exterior: ¡no matarás!) al ser humano y convertida, desde épocas muy antiguas, en un elemento de enfrentamiento, de fanatismo, de cruzada. Las cosas han cambiado: ahora el cristianismo resulta atacado brutalmente en muchos países musulmanes y el integrismo islámico, que deforma a su antojo los principios del Corán, constituye un flagelo, sobre todo para las mismas poblaciones musulmanas. La violencia interétnica en el seno del Islam es mucho más mortífera que el llamado «conflicto de civilizaciones». Hay, especialmente, un litigio entre un Islam más moderno y tolerante y otro más radical y fundamentalista. Ya lo escribió el teólogo Hans Küng: «no puede haber paz entre las naciones sin paz entre las religiones» [33].

Esta idea horizontal de la seguridad (que en inglés merece dos palabras: *security* y *safety* [34]) está relacionada, como apuntaba, con los demás valores esenciales de la comunidad internacional: la preservación del medioambiente, la protección de los derechos humanos, el progreso económico y social, etc. Aunque existe una general complementariedad entre estos valores, vamos a comprobar que las relaciones entre ellos en ocasiones son conflictivas. De todos los ámbitos interconectados con la paz y con la guerra voy a centrar mi atención en dos de ellos: el ámbito económico y el ámbito de los derechos humanos.

---

puede encontrar en *La sécurité internationale entre rupture et continuité. Mélanges Jean-François Guilhaudis*, Bruylant (2007). Esta sociedad de riesgo deriva tanto de accidentes como del mal uso, ilícito e intencionado, de materiales contemporáneos. El buen gobierno debe prevenir todas estas circunstancias. Véase, por ejemplo, el Plan estatal de Protección civil ante el riesgo químico. RD 1070/2012, de 13 de julio. BOE de 9.08.2012.

33. Véase Küng, H., *Proyecto de una ética mundial*, Barcelona (1994), págs. 98.

34. Y en francés otras dos: sécurité y sûreté.

El ámbito económico

Como en todos los órdenes de la vida pública, la economía juega también en materia de guerra y paz un papel primordial. A veces, las sanciones económicas que pretenden que un Estado belicoso capitule, se presentan como alternativa a una solución armada mucho más trascendente e imprevisible. Sin embargo, estas sanciones, si no son verdaderamente «inteligentes», pueden penalizar injustamente a la población dejando a sus dirigentes atrincherados en el poder. Ya apuntaba, por otra parte, arriba los pingües beneficios que se pueden extraer del negocio de la guerra. A su vez, ese mismo negocio es frecuentemente sufragado con el dinero procedente de actividades ilícitas (narcotráfico, contrabando de especies amenazadas de extinción…). En el derecho internacional económico, en fin, abundan las cláusulas que amparan una medida unilateral tomada por un Estado en aras de su seguridad nacional o internacional, de su orden público, etc.

Desde la óptica de los países pobres, huelga señalar el círculo vicioso en que se debaten muchos de ellos, atrapados entre la guerra y el hambre, que se retroalimentan. Como se suele decir, el hambre es la mayor arma de destrucción masiva. Incluso en países en paz, pero con un índice alto de crimen organizado, la delincuencia se presenta como una rémora para conseguir su progreso social (nuevamente los supuestos de Honduras o de Venezuela sirven de botones de muestra). Piénsese que la misión naval que la UE y otros países llevan a cabo en aguas cercanas a Somalia tiene por cometido, aparte de disuadir la piratería marítima, escoltar los suministros del Programa Mundial de Alimentos (PAM), tan obstaculizado y amenazado en su ejecución por la inseguridad reinante en ese castigado y fallido país. Piénsese también en el riesgo, desgraciadamente materializado en ocasiones, que corren los cooperantes internacionales en regiones sacudidas por conflictos armados.

La pobreza arrastra a la violencia, y viceversa. No sorprende, pues, que una parte de la cooperación internacional para el desarrollo vaya destinada a aliviar los estragos de un conflicto armado y a sentar las bases para el desarrollo autónomo y estable del

país [35]. En ocasiones, como se ha hecho en Afganistán, se compra directamente la entrega de las armas a los combatientes: se calcula que unos 1.300 talibanes han cambiado sus armas por dinero en Badghis, la provincia bajo control español. Es desazonador comprobar que en muchos territorios donde escasean los víveres primarios abundan, en cambio, armas y municiones para entrematarse. Algunos contendientes, incluidos los niños soldados, solo ven salida existencial en empuñar una metralleta y dispararla contra su circunstancial y muchas veces inopinado enemigo. Nunca falta un mercado donde aprovisionarse de artefactos letales. El negocio del miedo siempre funciona y el complejo industrial-militar se enriquece a costa de estas guerras sucias. Sin embargo, sería injusto, en todo caso exagerado, colegir de este estado de cosas que la injusticia social y la miseria son los únicos caldos de cultivo de la violencia mundial, a la que de alguna forma dan legitimidad. Este razonamiento se viene utilizando en relación con el terrorismo *yihadista*, y desde luego no está claro ni acreditado que la mayoría de estos integristas se rebelen contra la pobreza y la injusticia.

35. Como ejemplo de la práctica española, puede verse el Real Decreto 1948/2009, de 18 de diciembre, por el que se regula la concesión directa de una subvención a la Autoridad Intergubernamental para el Desarrollo (BOE de 19.12.2009). En su exposición de motivos se empieza leyendo lo siguiente: «Dentro de los objetivos prioritarios de la acción del Estado en el exterior se encuentra el fortalecimiento de la seguridad internacional y el apoyo a todas aquellas iniciativas, gubernamentales o de la sociedad civil, que contribuyan a crear las condiciones para reforzar la paz, la seguridad y la estabilidad internacionales». En consecuencia, se decide otorgar la subvención a la Autoridad Intergubernamental para el Desarrollo (IGAD), cuya sede social se encuentra en Yibuti y que desarrolla un importante papel de vehículo para el diálogo político y la seguridad del Cuerno de África. En el orden de la UE también ha sido reconocido este carácter expansivo de la seguridad y defensa, conectada con la cooperación para el desarrollo. Así se establece en la Sentencia del Tribunal de Justicia de la Unión de 20 de mayo de 2008. Asunto C-91/05. En esta resolución se afirma que la contribución económica que la Unión Europea hace en el marco de la moratoria sobre las armas ligeras y de pequeño calibre debe ser ubicada asimismo en la política de cooperación para el desarrollo, y no solo en la relativa a la política exterior y de seguridad, pues la Decisión correspondiente participa de ambos objetivos, sin que ninguno de ellos sea accesorio del otro.

La mayor y más desoladora paradoja en que se desenvuelven muchos de estos Estados fracasados es que la misma tenencia en su territorio de bienes naturales muy codiciados se convierte en un factor desencadenante o agravante de una guerra: es lo que se ha dado en llamar «la maldición de los recursos naturales». Podríamos hablar, en este sentido, de los «diamantes de sangre» en Sierra Leona, del coltán en la República Democrática del Congo o del petróleo en la frontera entre Sudán y Sudán del Sur. Cabe vaticinar nuevos conflictos en torno a las llamadas «tierras raras», metales indispensables para la producción de bienes de alta tecnología. De momento, este tema solo ha provocado entre China (principal productor) y la Unión Europea una guerra *comercial*, de las muchas que se dirimen en un contexto internacional globalizado y ferozmente competitivo. No se olvide que las consideraciones económicas se entreveran con las ecológicas (la *ecolonomy*). No es difícil vislumbrar conflictos por el aprovechamiento del agua, acaso el mayor problema securitario en un futuro no lejano, o la aparición de refugiados ambientales. Mientras tanto, el indiscutible cambio climático no produce ni frío ni calor a una gran parte de la ciudadanía…

Si la pobreza es estructural en numerosos países, el mundo rico está padeciendo una acusada crisis económica temporal, pero significativa de la nueva distribución de poder en el mundo, con las consecuencias geoestratégicas correspondientes. Hablaba antes de guerras comerciales. Pues bien, la guerra financiera ha irrumpido con toda crudeza, y de ello ha pasado a ocuparse en España el Centro Nacional de Inteligencia (CNI), en la certeza de que hay ataques especulativos contra la economía española y contra el euro. Las turbulencias económicas vienen provocando e imponiendo en la zona euro, y singularmente en países como Grecia, Portugal o España, una *economía de guerra* que aspira al control de la deuda soberana (no hagamos ahora caso, por supuesto, de la idea keynesiana de que un conflicto armado puede ser un revulsivo para una economía deprimida…). Es evidente, como la misma Directiva 1/2012 reconoce, que una deuda disparada supone un elemento de riesgo, de vulnerabilidad para un país, aunque ya están lejos los tiempos en que el cobro de las deudas contractuales entre países legitimaban la declaración de

guerra [36]. Es indudable que una crisis de estas dimensiones en el marco de una unión monetaria, que no económica todavía, hace al Estado menos autónomo, menos libre de su destino social, menos soberano.

El caso es que los sucesivos paquetes de recortes presupuestarios, así como en general el marco globalizado en que se desenvuelve la economía, ocasionan un debilitamiento de nuestro Estado social y democrático de Derecho y provoca una acentuada inseguridad laboral, vital. Es lo que el sociólogo Ulrich Beck ha llamado «la política económica de la inseguridad», en la cual ningún trabajo ni ningún conocimiento adquirido lo es para toda la vida, en la cual se piensa fundadamente que nuestros hijos pueden vivir peor que sus padres [37]. Naturalmente, este estado de cosas puede acabar amenazando la paz ciudadana al desdibujarse el pacto social en que estábamos sustentados.

Lógicamente, la partida de Defensa también está sufriendo recortes y ajustes, los cuales afectan tanto a la organización interna (reducción de tropas, inversiones…) como a las relaciones internacionales del departamento, pues España está implicada en distintos programas internacionales que conllevan importantes desembolsos en los próximos años (el avión de combate europeo —*Eurofighter*—, el sistema de aviones espía de la OTAN, etc.) [38]. Como suele decirse, se trata de alcanzar unas fuerzas armadas más reducidas, flexibles y baratas. Cabe solo pensar y desear que de los recortes presupuestarios no resulte una España

36. Fue el Tratado Drago-Porter, firmado en 1907, el primero que declaró ilegal la guerra por esta circunstancia.

37. Véase Beck, U., «La política económica de la inseguridad», *El País*, de 27.05.2012. Este autor, a lo largo de su fecunda obra, nos ha explicado la «sociedad del riesgo» en la que vivimos y ha apostado por un «realismo cosmopolita» Véase, en este último sentido, Beck, U., *La mirada cosmopolita o la guerra es la paz*, Paidós (2005).

38. Cfr. el Real Decreto-Ley 26/2012, de 7 de septiembre, por el que se concede un crédito extraordinario en el presupuesto del Ministerio de Defensa para atender al pago de obligaciones correspondientes a programas especiales de armamento por entregas ya realizadas. BOE de 8.05.2012. Este Decreto-ley fue convalidado en el Congreso de los Diputados el 20 de septiembre siguiente.

peor defendida y menos implicada en la seguridad colectiva con sus socios [39].

El ámbito de los derechos humanos

Acabamos de hablar del deterioro que para los derechos y libertades fundamentales comporta el actual caos en que está sumida la economía internacional. Más allá de esta circunstancia, las conexiones entre los conflictos propiamente armados y la protección de los derechos humanos tienen otras muchas caras, que aquí someramente espigaré.

Desde luego, la relación más clásica entre la guerra y la dignidad humana se encuentra en el llamado *ius in bello*, del que se encuentran manifestaciones muy antiguas, y que, en esencia, imponen librar la batalla sin causar males superfluos ni sufrimientos innecesarios, procurando no ir más allá de lo que sea estrictamente preciso para doblegar la resistencia del enemigo. Es indudable que en los últimos siglos, y en especial en la última centuria, hemos asistido a una mayor regulación y control del derecho humanitario bélico con instrumentos innovadores como la justicia penal internacional y tratados que tienden a prohibir la fabricación y el empleo de las armas químicas o de las minas antipersonas. Son instituciones muy beneficiosas que previenen o combaten el flagelo del conflicto armado. Sin embargo, es indudable que muchos conflictos actuales se siguen desarrollando con una crueldad inusitada. Desgraciadamente, también en la industria del ocio (cine, videojuegos…) se sigue banalizando y hasta glorificando la violencia armada, el pisoteo de la dignidad humana. La guerra no es divertida ni hilarante. Es indudable que el derecho humanitario bélico sigue teniendo agujeros negros en su formación y, sobre todo, en sus mecanismos de garantía [40]. Esto hace que a

39. Véase Fernández Sola, N., «El impacto de la reducción de los presupuestos de defensa en España sobre la participación en la política común de seguridad y defensa», *Cuadernos aragoneses de economía*, (2012), págs. 49-64.

40. Cassese, en su libro general de Derecho internacional, llegó a señalar que el derecho humanitario de los conflictos armados era la rama más vulnerable de este ordenamiento jurídico, el cual, en estas cuestiones, se limitaba a menudo a poco más que «to mirror the constellation of powers of the world community», véase Cassese, A., *International Law in a Divided World*, New York (1986), pág. 285.

menudo el Consejo de Seguridad de la ONU, ante su incapacidad para detener el conflicto, se centre en paliar los estragos humanitarios que causa. No soslayemos, por otra parte, que el derecho de los conflictos armados no solo procura atenuar los daños para las personas, sino también para otros bienes, como el medioambiente o el patrimonio cultural, dignos de protección.

Las Fuerzas Armadas españolas, en los tres decenios largos de democracia, han representado, con las excepciones propias de toda organización humana, un modelo de sumisión a la normativa interna e internacional de salvaguarda de los derechos humanos, de respeto a la autoridad civil, cumpliendo y haciendo cumplir en el territorio nacional y exportando a terceros países los valores constitucionales. Sus actuales ordenanzas imponen a sus miembros velar por el cumplimiento de los derechos humanos aun fuera de España y sin que el principio de «obediencia debida» pueda servir de eximente [41]. Es indudable que hemos asistido a un proceso, en todos los órdenes, de *humanización* del Ejército, aunque evidentemente no es ni debe convertirse en una ONG. La misma integración de la mujer es un elemento alentador, y no solo porque se predica de la fémina un mayor espíritu pacifista que del varón…

Por lo demás, está fuera de duda la complementariedad jurídica y axiológica que debe reinar entre la paz y los derechos humanos, y de estos dos valores con otro con el que forman una triada inextricable: el progreso social de los pueblos. Tengamos en cuenta que a estos principios estructurales se adiciona el de la autodeterminación de los pueblos a los que el Derecho internacional les reconoce el derecho de elegir su propio estatuto (el

41. Estas Reales Ordenanzas para las Fuerzas Armadas están recogidas en el Real Decreto 96/2009, de 6 de febrero (BOE de 7.02.2009), y son extensibles a la Guardia Civil, según establece el RD 1437/2010, confirmado, sobre la base del carácter militar de este Cuerpo, por la Sentencia del Tribunal Supremo (Contencioso-Administrativo) de 13.02.2012. Más allá de un nutrido cuerpo normativo en esta rama del Derecho internacional oponible a España, puede citarse también la existencia de la Comisión Española de Derecho Internacional Humanitario, cuyo Real Decreto de constitución (el 1513/2007, de 16 de noviembre) figura publicado en el BOE de 26.11.2007.

saharaui, el palestino…). Ahora bien, los movimientos secesionistas son, con frecuencia, una fuente de convulsión y violencia internacionales, pues replantear el mapa político suele estar bañado en sangre y provocar Estados fallidos. De hecho, desde la sociedad civil se viene trabajando, con algún reconocimiento ya en el campo diplomático, en la codificación de un derecho humano a la paz [42]. Más allá de la perspectiva de los derechos humanos, es inobjetable que un régimen democrático representa un indicio más fiable que uno dictatorial de sociedad abierta y armoniosa en las relaciones internas e internacionales. Resulta lógico, pues, que el derecho post-bélico suela incluir la organización y la supervisión de elecciones libres para dotar al país fallido de un gobierno estable y representativo (si bien, es verdad, que a veces los procesos electorales enconan aún más la situación, sobre todo cuando no se reconocen unánimemente los resultados oficiales).

Sin embargo, las relaciones entre estos valores primordiales de la comunidad internacional no siempre son armoniosas. Piénsese, por poner un caso bien de nuestros días, en la necesidad, pero a veces dificultad, de conciliar los principios de seguridad y de libertad en la lucha contra el terrorismo internacional. El escritor alemán decimonónico Goethe escribió que prefería una injusticia a un desorden. Si se lee y se interpreta a la luz de su tiempo la Carta de San Francisco se podría decir, y reprochar, que la paz estaba por encima de cualquier otro objetivo, incluso cuando se trataba de una paz injusta. En realidad, seguridad y libertad son valores complementarios y no antagónicos. Ya dijo Montesquieu que libertad era la sensación que cada cual tenía de su propia seguridad. En nuestros días, significativamente, la Carta de Derechos Fundamentales de la Unión Europea, en su artículo 6, ensambla ambos conceptos al decir que «Toda persona tiene derecho a la libertad y a la seguridad». No se trata de que la derecha política se apropie del valor «seguridad» y de que la izquierda política reivindique para sí el valor «libertad». Es deplorable, desde luego, que los grupos reaccionarios y radicales en el mundo

42. Véase Rueda Castañón, C.R., Villán Durán, C., (eds.), *La Declaración de Luarca sobre el derecho humano a la paz*, Ediciones Made, Granda-Siero (2007).

árabe aprovechen los aires de libertad de la llamada «primavera» para sembrar el terror. No está claro, ni mucho menos, que el fundamentalismo islámico haya resultado perdedor de las revueltas de los últimos tiempos contra los dictadores prooccidentales.

De ahí que en la práctica internacional reciente se haya acuñado, aunque con una interpretación y aplicación erráticas, un derecho de injerencia humanitaria y hasta la responsabilidad de proteger a una población asediada, frecuentemente por su propio gobierno, que puede convertirse en el principal enemigo de sus ciudadanos, así como la comunidad internacional puede convertirse en la principal tabla de salvación para ellos. Desde este punto de vista habría guerras a favor y en contra del Derecho internacional, que suele ser manipulado en estos procesos, eminentemente políticos. Naturalmente, en ocasiones la intervención es lícita cuando la solicita el propio Gobierno ante la insurrección interna. Pero, ¿se puede hacer uso de la fuerza armada en nombre de un bien superior como es la preservación del derecho a la vida y a la libertad de un pueblo masacrado? La pregunta, como se sabe, abre un amplio dilema moral, político y jurídico, que no tiene una respuesta apodíctica. De hecho, la práctica internacional ofrece dobles raseros a la hora de valorar esa llamada responsabilidad de proteger, y al proteger [43]. En algunos países, como en Egipto, el factor securitario a los ojos occidentales tiene más importancia que el factor libertario. Aunque ambos factores deben complementarse, no siempre lo hacen; en ocasiones la apertura política puede entrañar más desorden y hasta más represión, como a lo peor la *primavera árabe* puede terminar produciendo en algún país. Cada caso en concreto tiene sus propias particularidades, de forma que la respuesta debe ser casuística, aunque siempre ponderando las necesidades humanitarias. Es verdad que los intereses predominan sobre los valores, pero no siempre es posible, ni conveniente, ordenar la intervención militar, sobre todo cuando no se sabe a ciencia cierta si los insurgentes tienen verdaderos propósitos libertadores o si la

43. Véase Ferrer Lloret, J., «La Unión Europea y la responsabilidad de proteger», en González Alonso, L-N., *La Unión Europea: el multilateralismo eficaz. ¿Un compromiso consistente con Naciones Unidas?*, Iustel (2012), págs. 217-268.

diplomacia (acompañada de sanciones de naturaleza no militar) aún tiene recorrido antes de llegar a la fuerza armada, que debe ser, en todo caso, una última ratio, pues siempre conlleva daños colaterales, aparte de los frontales, y siempre se cometen por ambas partes crímenes contra la humanidad. Desde el punto de vista que más interesa a este trabajo no podemos soslayar que la respuesta adecuada no debe emanar solo de los políticos o los intelectuales, sino que debe basarse en una ponderación de las circunstancias llevada a cabo desde el propio orden militar, pues de una estrategia militar se trata. En fin, nos encontramos, como digo, ante una cuestión vidriosa, que quizá solo con la perspectiva del tiempo puede ser analizada: ¿Mereció la pena para los derechos humanos y la pacificación de la región la intervención armada en Kosovo? ¿Y la intervención en Irak o en Afganistán? Pero probablemente el tiempo tampoco puede dilucidar el dilema, sino que hay que recurrir a la historia *contrafactual*, y eso es un ejercicio de política-ficción: ¿qué habría pasado sin la política de apaciguamiento hacia Hitler? ¿Qué habría pasado en Irak y en la región con la permanencia de Saddam Hussein en el poder? En todo caso, la profanación de cadáveres llevada a cabo repulsivamente por soldados norteamericanos o la lapidación aún de mujeres adúlteras en Afganistán, prácticas tan reprobables, no deben empañar otros logros que puede haber traído consigo la misión militar en aquel castigado país.

Un nuevo perfil de los ejércitos

A consecuencia de los cambios ocurridos en la seguridad internacional, es común hablar de una cierta desmilitarización de sus coordenadas actuales, también en el marco de una cierta deshumanización de los conflictos bélicos (ciberseguridad, robots, aviones no tripulados…). Es verdad, como superficialmente hemos apuntado, que la seguridad es un campo ahora polivalente, interdisciplinar: hay nuevas formas de violencia, nuevos miedos, nuevos instrumentos (y no solo armas) para preservar la seguridad, para combatir la inseguridad [44]. También es evidente que a

44. Cfr. Torres Cazorla, M.I., García Rico, E.M., (coords.), *La seguridad internacional en el siglo XXI. Nuevas perspectivas*, Plaza & Valdés, (2011).

los ejércitos se les encomiendan nuevos cometidos y responsabilidades. La frase acuñada «boots on the ground» testimonia una visión de la función castrense más pegada a la tierra, más mezclada con la ciudadanía. En algunos países, sobre todo del área latinoamericana, se le vienen confiando funciones más vinculadas a la seguridad ciudadana, como la lucha contra el narcotráfico y, en general, el crimen organizado, haciendo que las tropas patrullen las ciudades aun en tiempos de paz (aunque, desde luego, de feroz delincuencia). En España, sin ir más lejos, las funciones asignadas a la Unidad Militar de Emergencias se desarrollan en el ámbito internacional (como en Haití), pero particularmente dentro del territorio nacional [45]. Todo ello es un signo de los tiempos que corren, en los cuales lo interno y lo internacional están estrechamente imbricados. Piénsese igualmente en el caso excepcional de Alemania, cuyo ejército solo ha sido autorizado, y en casos extraordinarios, a desplegarse en el interior del país mediante una Decisión de su Tribunal Constitucional de agosto de 2012.

En nuestro contexto occidental asistimos a una reducción del gasto militar y a una remodelación de los ejércitos. La crisis económica desde luego empuja en este sentido, pero también una escasa cultura de la defensa entre nosotros, de modo que la partida presupuestaria en este campo no es tan alentada como en educación, justicia o sanidad, pongo por casos. Digamos que no es un reclamo electoral, un eslogan político, cosa criticada desde el Pentágono hacia Europa por su ventajismo e ingenuidad. Desde luego, este estado de cosas refuerza la necesidad de cultivar el multilateralismo con nuestros socios, de practicar lo que se ha dado en llamar una «defensa inteligente», la cual no termina de ser enfatizada convenientemente en la nueva Directiva de la Defensa Nacional de 2012. En cualquier caso, el compromiso está claro: conseguir un sistema de disuasión eficaz y creíble, pero sin abandonar nuestros compromisos —e intereses— internacionales. De nuevo: lo interno

45. Como otra faceta de su vertiente internacional, se puede señalar que esta Unidad está especialmente implicada en el Acuerdo entre los Gobiernos del Reino de España y de la República Francesa en el ámbito de las Situaciones de Emergencia y de Protección y Seguridad Civiles. BOE de 11.09.2012.

y lo internacional van de la mano. Además, en lo que se refiere a Europa, los propios ajustes económicos decretados en nuestro gran aliado y protector (Estados Unidos), así como una mayor orientación de la aún superpotencia hacia el Asia-Pacífico, postergan el valor geoestratégico del Viejo, y envejecido, Continente. Saquemos la conclusión optimista: Europa ya no es un teatro de operaciones tácticas como lo fue durante la Guerra Fría (aunque no dejan de cernirse amenazas de distinta índole sobre su población).

Sin embargo, dejando a un lado las oportunidades que brinda el complejo industrial-militar, está fuera de duda que las Fuerzas Armadas siguen siendo en todas partes un elemento de poder, de prestigio o de intimidación, un indicio por sus características de la política internacional que pretende llevar a cabo el Estado, un corolario necesario de su acción exterior. Precisamente, una de las penalidades que padece la política exterior de la Unión Europea es la inconcreción y las fracturas que han lastrado su política de seguridad y defensa, mejorada sin embargo en los últimos años. Es revelador también que Estados ahora fallidos como Afganistán o Libia pretendan, esencialmente, recomponer unas fuerzas de seguridad propias, sólidas y unificadas.

Que el sistema defensivo de un Estado es un elemento asociado a su peso económico, a la «marca país», lo prueba que los países emergentes, en paralelo a su ascenso económico, vienen dotándose de un aparato militar más potente. Es, ciertamente, el caso de Rusia, cuyas aspiraciones de mantenerse como la potencia estratégica que fue antaño, pasan inevitablemente por agrandar, y ostentar, su músculo militar, un cierto «ardor guerrero» que una buena parte de la población parece agradecer y aplaudir en Vladímir Putin; y la población que discrepa de este jerarca se expone precisamente a sufrir ese músculo represor.

Ya hemos hablado, por otra parte, del llamado «ascenso pacífico» de China, que contagia su escalada militar (no se sabe si más empujada por los disidentes internos o por los desafíos exteriores) a la región circundante. El caso de Brasil, desde luego mucho menos inquietante, es parecido, aunque en Sudamérica son la política y los exabruptos chavistas, «bolivarianos» los que crean cierto desasosiego en su entorno.

El supuesto de Venezuela, como el de Irán con su amenazante programa nuclear, corrobora algo distinto: algunos gobiernos prefieren privar a sus ciudadanos de bienes primarios a cambio de enarbolar la bandera de la soberanía militar frente a potencias exteriores. Ya se sabe que en Irán sus instalaciones nucleares son exhibidas como un elemento de orgullo nacional y de tapadera de los problemas cotidianos de la población.

En Corea del Norte, el factor militar es más decisivo: no se trata solo de sostener al abominable régimen estalinista, que mantiene en la hambruna a gran parte de sus habitantes, sino de mantener con vida artificial al Estado frente a una eventual reunificación con sus vecinos, prósperos y democráticos, del Sur.

La verdad es que las Fuerzas Armadas siguen desempeñando un papel importante, aunque de muy distinto valor, entre los países. Las asonadas militares siguen, patéticamente, retumbando en algunos países africanos (Mauritania, Guinea Bissau, Malí…). En cambio, y felizmente, los cuartelazos se han apagado bastante en América Latina (algunas maniobras políticas inconstitucionales, como las producidas en Paraguay y sobre todo en Honduras, han provenido formalmente más del ámbito civil que del castrense). Algunos dirigentes del hemisferio americano aún siguen procediendo del mundo militar, aunque como autoridades civiles resultantes de comicios, como Chávez en Venezuela o Humala en el Perú, y el caudillismo del primero es patente, si bien es esa una característica nada rara en la región, aun entre dirigentes civiles y elegidos en procesos electorales. El caso de la Cuba castrista merecería un epígrafe aparte… Esperemos que en este país, como está sucediendo tímidamente en otros como la antigua Birmania, el ejército impulse el cambio hacia una sociedad abierta y no siga *bunkerizando* tristemente a la población.

Lo cierto es que la influencia del Ejército en la vida civil no es privativa de los regímenes formalmente castrenses. Muchas democracias incipientes o nominativas, como la de Egipto o la de Pakistán, siguen estando custodiadas, intervenidas por las Fuerzas Armadas. De este país asiático se ha llegado a decir que es un ejército que posee un país. Paradójicamente, a las democracias occidentales les tranquiliza más esta democracia tutelada que una liberación auténtica de las fuerzas y aspiraciones ciudadanas. Con

motivo de la llamada *primavera árabe* algunos ejércitos, como el egipcio, se negaron a disparar contra su propio pueblo, mientras otros ejércitos, como el sirio, ejecutan una matanza sin piedad (aunque con algún desertor). No soslayemos algún otro caso peculiar, como el de las milicias turcas, encargadas por mandato constitucional de asegurar la aconfesionalidad del Estado, lo que supone un elemento tranquilizador contra las pulsiones integristas. En cualquier caso, el poderío de un ejército unificado es preferible a una multiplicación caótica de milicias que dan lugar a un Estado fallido que exporta su miseria y su desgobierno al conjunto de la región, y a veces más allá.

En el caso de nuestro país, donde la competencia de Defensa es lógicamente estatal [46], las Fuerzas Armadas, represoras otrora del poder civil, han desplegado en los años de democracia una brillante labor interna y externa, siendo esta última, la consistente en misiones de mantenimiento de la paz, de *nation-building*, uno de los mejores activos, un indiscutible *poder blando*, que aún conserva la deteriorada imagen de España. Se trata de prevenir, y no de provocar ni librar una guerra, dentro ni allende de nuestras fronteras. Así las cosas, ejército y pacifismo no están reñidos, sino que pueden y deben ser fuerzas convergentes, lo mismo que deben serlo la milicia y el espíritu humanitario.

En todo caso, los mejores tiros son los que se disparan contra la portería del adversario en los campos de fútbol, teatro de operaciones hoy en día de aspiraciones patrióticas. El lenguaje castrense que impregna al balompié es siempre bienvenido: asedio al área, bombardeo a la portería, fusilar al portero… Sin embargo, molesta que los arietes (también llamados artilleros o *killers*) a menudo tengan la pólvora mojada.

46. La estructura orgánica básica del Ministerio de Defensa se encuentra actualmente contenida en el Real Decreto 454/2012, de 5 de marzo. BOE de 6.03.2012.

Parte II

LEGISLACIÓN DE LAS ACTIVIDADES Y USO RESPONSABLE DE INTERNET

EL DERECHO INTERNACIONAL E INTERNET

Antonio Segura Serrano [*]

Introducción

Dada la naturaleza «virtual» de su existencia, la primera discusión jurídica importante a cerca de Internet se centró en su resistencia natural a la regulación. Desde los inicios de Internet, se produjo un debate que puede ser denominado como «regulación *versus* desregulación» con respecto a este nuevo campo de actividad [1]. ¿Es posible y factible regular Internet, o por el contrario, es Internet un lugar esencialmente libre, una *terra nullius* virtual? La posición libertaria fue abrazada por algunos académicos, especialmente en los EE.UU., durante los años noventa [2]. La soberanía del ciberespacio es la idea central en los escritos seminales como los de Johnson y Post. En su opinión, no sólo es imposible o inútil todo intento del Estado por regular Internet, sino que además es deseable que la red esté libre de la regulación estatal [3], ya que el

[*] Profesor Titular de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Granada.

1. Véase Gibbons, Llewellyn Joseph, «No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace», *Cornell Journal of Law & Public Policy*, vol. 6 (1997), pág. 499, que sostiene que «[t]he regulation of cyberspace may take one of three forms. Cyberia will be government regulated, self-regulated, or even unregulated».

2. Se ha convertido en un lugar común citar a John Perry Barlow como uno de los mayores promotores de la independencia del ciberespacio, véase Barlow, John Perry, *A Declaration of the Independence of Cyberspace*, en http://www.eff.org/~barlow/Declaration-Final.html; véase también Delacourt, John T., «The International Impact of Internet Regulation», *Harvard International Law Journal*, vol. 38 (1997), pág. 208, que subraya que hay argumentos sólidos a favor de una completa no regulación.

3. Véase Johnson, David R. y Post, David, «Law and Borders – The Rise of Law in Cyberspace», *Stanford Law Review*, vol. 48 (1996), pág. 1367; Post, David G., «Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace

autogobierno puede materializar mejor las ideas democráticas liberales [4].

Sin embargo, las reivindicaciones libertarias han sido impugnadas, tanto en el frente descriptivo [5], como en el normativo [6]. En primer lugar, es discutible si en realidad el ciberespacio constituye un lugar libre, una jurisdicción soberana, lejos del alcance del Estado [7]. En segundo lugar, aun dando por sentada esta suposición, lo que Internet es en realidad puede diferir de lo que debería ser, como han argumentado autores destacados como Lessig [8]. Goldsmith, en una obra ya seminal, ha utilizado la palabra «ciber-anarquía» para describir (y luchar contra) el tipo de discurso que defiende un espacio separado del mundo real y carente de reglas [9]. En agudo contraste con la visión separatista,

(article 3)», *Journal of Online Law*, 1995, en http://www.wm.edu/law/publications/jol/articles/post.shtml; Trotter Hardy, I. «The Proper Legal Regime for 'Cyberspace'», *University of Pittsburgh Law Review*, vol. 55 (1994), pág. 993, que promueve el uso de normas de «autorregulación», incluyendo mecanismos como la auto-ayuda, contratos, asociaciones privadas y la costumbre; Perritt, Henry H. Jr., «Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalist?», *Berkeley Technology Law Journal*, vol. 12 (1997), pág. 419, que señala que el autogobierno es deseable en el marco de las comunidades electrónicas.

4. Véase Post, David G., «Governing Cyberspace», *Wayne Law Review*, vol. 42 (1996), pág. 170-171; Post, David G., «The «Unsettled Paradox»: The Internet, the State, and the Consent of the Governed», *Indiana Journal of Global Legal Studies*, vol. 5 (1998), pág. 535-542. *Contra* Netanel, Neil W. «Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory», *California Law Review*, vol. 88 (2000), pág. 488; Sylvain, O., «Internet Governance and Democratic Legitimacy», *Federal Communications Law Journal*, vol. 62 (2010), pág. 205.

5. Véase Wu, Timothy S., «Cyberspace Sovereignty? – The Internet and the International System», *Harvard Journal of Law & Technology*, vol. 10 (1997), pág. 647.

6. Véase Lessig, Lawrence, *Code and Other Laws of Cyberspace*, 1999, 25.

7. Véase Wu, Timothy S., «Cyberspace Sovereignty?...», *loc. cit.*, pág. 649-656; Trachtman, Joel P., «Cyberspace, Sovereignty, Jurisdiction, and Modernism», *Indiana Journal of Global Legal Studies*, vol. 5 (1997/98), pág. 562, que señala que «[t]he argument that technological changes occurring today require the death of the state and its regulatory function proves too much».

8. Véase Lessig, Lawrence, *Code and Other Laws of Cyberspace, op. cit.*, pág. 25.

9. Véase Goldsmith, Jack L., «Against Cyberanarchy», *University of Chicago Law Review*, vol. 65 (1998), pág. 1199.

los que pueden ser llamados tradicionalistas afirman que la institución política y jurídica conocida como el Estado es el organismo regulador apropiado para llevar a cabo la tarea de reglamentar Internet [10]. Además, lo cierto es que se han erigido normas en todo el mundo con el objetivo y el efecto de someter a Internet a una regulación «real» [11].

No obstante, teniendo en cuenta el carácter global de Internet, el Derecho internacional puede ser un instrumento más adecuado para la regulación de alguna de las diversas cuestiones que se plantean en este ámbito [12]. El presente análisis, por lo tanto, tiene como objetivo estudiar el papel actual de las normas internacionales relativas a la regulación de esta materia. Este ejercicio permitirá identificar los diferentes enfoques nacionales más importantes en la regulación de Internet, así como los instrumentos de Derecho internacional que resultan a partir de esos enfoques.

Hay un abanico de cuestiones relacionadas con esta nueva tecnología que las normas nacionales han afrontado de diversas formas. Algunos de los temas más importantes son la libertad de expresión frente a la lucha contra los contenidos nocivos; la protec-

10. Véase Goldsmith, Jack L., «The Internet and the Abiding Significance of Territorial Sovereignty», *Indiana Journal of Global Legal Studies*, vol. 5 (1998), pág. 476; Fried, Charles, «Perfect Freedom or Perfect Control?», *Harvard Law Review*, vol. 114 (2000), pág. 621; véase también Stein, Allan R., «The Unexceptional Problem of Jurisdiction in Cyberspace», *International Lawyer*, vol. 32 (1998), pág. 1174, que sostiene, con relación al Derecho del Ciberespacio, que «[w]hatever connections the Internet facilitates among its users, it has no claim of authority over them. Whatever difficulties territorial states have in regulating elusive Internet behavior, there is no Internet sovereignty with which they must reckon».

11. Ello ha conducido a una proliferación de las denuncias sobre censura y recorte de las libertades que existían en Internet en su estadio inicial, véase Froomkin, A. Michael, «Lessons Learned Too Well», *Miami Law Research Paper Series 2011-29*, pág. 3, en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1930017; Bambauer, Derek E., «Orwell's Armchair», *University of Chicago Law Review*, vol. 79 (2012), pág. 863.

12. Véase Heverly, Robert A., «Breaking the Internet: International Efforts to Play the Middle Against the Ends – A Way Forward», *Georgia Journal of International Law*, vol. 42 (2011), pág. 1083, que propone la creación de una nueva organización internacional para Internet.

ción de los derechos de propiedad intelectual frente a la piratería y la promoción de la información de dominio público; y el derecho a la privacidad y la protección de los datos personales frente al uso comercial de esos datos. Aunque hay otras posibles cuestiones que se pueden debatir (la educación, la seguridad cibernética, la fiscalidad, el comercio electrónico, etc.), los problemas anteriormente mencionados ofrecen una buena medida de las diferencias entre las legislaciones nacionales, y ponen de manifiesto el papel actual del Derecho internacional con respecto a Internet.

No obstante, existen algunas cuestiones tradicionales del Derecho Internacional relacionadas con Internet que no han atraído suficientemente la atención hasta ahora y que podrían hacerlo en el futuro [13]. En primer lugar, parece claro que la integridad de los servicios que permiten o dependen del buen funcionamiento de Internet es un asunto de seguridad nacional para cualquier país. Por lo tanto, habría que determinar si un ataque cibernético, en forma de un virus o de otro modo, puede ser considerado como un ataque armado, y si es así, si tal ataque puede jurídicamente desencadenar la legítima defensa de un país, o hacer incluso que se ponga en marcha la acción colectiva de las Naciones Unidas (ONU).

En segundo lugar, debido a que Internet es importante no sólo para cada uno de los países de la Comunidad Internacional, sino también porque es crucial para el bienestar de las personas tanto en los países desarrollados como en desarrollo, parece adecuado preguntarse sobre la gobernanza de Internet. Desde el Derecho Internacional se puede contribuir al debate mediante la introducción de un concepto muy interesante, el relativo al Patrimonio Común de la Humanidad. El análisis de este concepto puede ser útil para responder a varias preguntas, como quién gobierna Internet, o quién tiene derecho a apropiarse de Internet, y cómo debe ser gobernado Internet.

Por último, se podría plantear si el acceso a Internet puede ser considerado como un derecho humano. Está claro que la

13. Véase Segura Serrano, Antonio, «Internet Regulation and the Role of International Law», *Max Planck Yearbook of United Nations Law*, vol. 10 (2006), pág. 191.

libertad de expresión es un derecho fundamental. El acceso a Internet, sin embargo, significa mucho más que la libertad de expresión, ya que implica temas que van desde la educación hasta la participación política. En este sentido, ya se han adoptado algunas medidas en el plano nacional con el fin de esbozar el denominado derecho al «acceso universal», que podría incluir el derecho de acceso a Internet (por ejemplo, Finlandia ha reconocido en 2010 el derecho humano fundamental a Internet de banda ancha).

Algunas de estas problemáticas relacionadas con Internet ya se han abordado desde el plano internacional con ocasión de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), celebrada en Ginebra en 2003 [14] y en Túnez en 2005 [15], patrocinada por las Naciones Unidas y la Unión Internacional de Telecomunicaciones (UIT). El objetivo de la CMSI es el de establecer los principios operativos que permitan materializar la democracia y la justicia en este ámbito.

Libertad de expresión *versus* contenidos nocivos

En primer lugar, la voluntad por parte de algunos Estados (en especial los países europeos) por controlar y eliminar contenidos nocivos en Internet ha chocado con el firme y constitucionalmente protegido derecho a la libertad de expresión en los Estados Unidos. Mientras que en EE.UU. hay un sentimiento fuerte, protegido por la Constitución, que favorece la libertad de expresión, los países europeos y Australia son más favorables, en general, hacia el control de la distribución de contenidos nocivos.

El Derecho Internacional tiene un papel importante que desempeñar con respecto a este problema de fondo, porque ésta también es una cuestión de competencia. Los conflictos regula-

14. Cumbre Mundial sobre la Sociedad de la Información, *Declaración de Principios, Construir la Sociedad de la Información: Un Desafío Global para el Nuevo Milenio*, Ginebra, 12 de diciembre de 2003, Documento WSIS-03/GENEVA/4-S, de 12 de mayo de 2004.

15. Cumbre Mundial sobre la Sociedad de la Información, *Compromiso de Túnez*, Túnez, 18 de noviembre de 2005, Documento WSIS-05/TUNIS/DOC/7-S, de 28 de junio de 2006.

torios en el ciberespacio están frecuentemente ligados a la interacción entre, por un lado, la disponibilidad en todo el mundo en la web de los datos que se consideren dañinos u ofensivos a los valores fundamentales en el Estado que ejerce jurisdicción, y por otro lado, las protecciones constitucionales a la libertad de expresión que existen en el Estado en el que los datos se hacen accesibles, es decir, los EE.UU., donde se encuentran muchos de los proveedores de servicios de internet.

Varios asuntos, como el relativo a *Compu Serve* y *Yahoo! Francia* demuestran el enfoque europeo seguido por Alemania y Francia sobre esta cuestión.

El caso *CompuServe*[16] fue uno de los primeros y más conocidos casos que planteaba un «auténtico» conflicto normativo[17]. El presunto delito para el Derecho alemán, el Código Penal, consistió en el suministro por *CompuServe Deutschland* (una subsidiaria 100 % de *CompuServe EE.UU.*) de acceso público a contenido violento, pornografía infantil y bestialismo. El contenido se almacenaba en los servidores de grupos de noticias de *CompuServe* en EEUU. Después de bloquear el acceso a dicho contenido en todo el mundo, *CompuServe* puso software de control parental disponible para sus suscriptores y desbloqueó los grupos de noticias. Sin embargo, un tribunal de Múnich dictó una sentencia contra uno de los directores generales de *CompuServe Deutschland*[18]. Aunque el caso fue posteriormente anulado

16. Véase Amtsgericht München (Tribunal de Primera Instancia de Munich), *NJW* 51 (1998), pág. 2836.

17. Véase Watt, Horatia Muir, «Yahoo! Cyber-Collision of Cultures: Who Regulates?», *Michigan Journal of International Law*, vol. 24 (2003), pág. 676, que subraya que «[t]ypically, an assertion of freedom of expression in the state in which the website is located clashes with restrictive legislation in the receiving state, designed to protect such values as the right of privacy, to restrict hate speech or libel, or to prohibit indecency or pornography. The free availability of information collides with the negative right of the receiving state to protect itself against outside interference».

18. Véase Grainger, Gareth, «Freedom of Expression and Regulation of Information in Cyberspace: Issues concerning Potential International Cooperation Principles», en Fuentes Camacho, Teresa (ed.), *The International Dimensions of Cyberspace Law,* 2000, pág. 90-91.

por un tribunal superior alemán [19], esta sentencia atrajo muchas críticas, especialmente desde los EE.UU.

Estas críticas fueron escasas, sin embargo, en comparación con la casi universal condena recibida por el caso *Yahoo!* en EE.UU. Este caso surgió cuando dos grupos franceses de interés público, *La Ligue Contre le Racisme et L'Antisémitisme* (LICRA) y *L'union des Étudiantes Juifs de France* (UEJF), demandaron a *Yahoo! Inc.*, una corporación de Delaware ubicada en California. El hecho presuntamente delictivo fue la puesta a la venta de objetos nazis por el sitio web de subastas *Yahoo!* accesible en Francia, que fue considerada ilegal según el Derecho francés. En efecto, la legislación francesa, junto con otras muchas leyes nacionales, puede ser considerada como conforme con la Convención sobre la Eliminación de todas las Formas de Discriminación Racial (CEDR) de 1965. Los reclamantes solicitaron una orden de prohibición a *Yahoo!* para que no mostrase estos objetos de exaltación en Francia.

El tribunal francés, que estimó que tenía jurisdicción personal debido a que el daño fue causado en Francia, solicitó un dictamen pericial sobre la posibilidad que tenía *Yahoo!* de bloquear el acceso a los usuarios franceses, en vez de eliminar completamente el contenido del sitio web en todo el mundo. Después de haber sido informado de que esto se podría lograr con un éxito del 90 por ciento (además, los usuarios franceses eran recibidos por el sitio web con anuncios en francés, lo que significaba que algún tipo de identificación geográfica ya estaba disponible), el tribunal ordenó a *Yahoo!* «tomar todas las medidas a su disposición, para disuadir y hacer imposible toda visita a *Yahoo.com* para participar en el servicio de subasta de objetos nazi» [20]. Después de eso, *Yahoo!* pretendió obtener una sentencia por la que la decisión francesa no pudiera

19. Véase LG München (Tribunal de Apelación de Munich), *NJW* 53 (2000), pág. 1051. Aparentemente, el juez de instrucción en el asunto *CompuServe* no aplicó adecuadamente al caso la legislación sobre Internet, véase Determann, Lothar «Case Update: German CompuServe Director Acquitted on Appeal», *Hastings International & Comparative Law Review*, vol. 23 (2000), pág. 112.

20. Véase LICRA & UEJF v. Yahoo! Inc., T.G.I. Paris, 22 de Mayo de 2000, *Dalloz* 2000, info rapides pág. 172.

ser reconocida en los EE.UU. El Tribunal de Distrito de EEUU, además de considerar que tenía jurisdicción, sentenció sobre el fondo a favor de *Yahoo!*[21] Sin embargo, la Corte de Apelaciones de EE.UU. posteriormente revirtió esa decisión[22], y sostuvo que el Tribunal de California no tenía jurisdicción personal sobre las partes francesas y que Francia tenía todo el derecho a declarar a *Yahoo!* responsable en Francia[23].

Pese a las críticas abrumadoras que la decisión francesa recibió en los EE.UU., el caso *Yahoo!* demostró que los instrumentos tradicionales de conflicto de leyes pueden aplicarse al ciberespacio, y que Francia tenía derecho a aplicar su legislación nacional, ya que los efectos perjudiciales se habían producido en su territorio[24]. El caso también confirmó que en los litigios transfronterizos en que surgen cuestiones de libertad de expresión, no es el lugar del país del proveedor de la información, sino el lugar del país del destinatario el que rige la situación[25]. El caso *Gutnick*, decidido por el Tribunal Supremo australiano[26], vino a corroborar

21. Véase Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 145 F. Supp. 2d 1168-1181 (N.D. Cal. 2001).

22. Véase Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 379 F. 3d 1120-1126 (9th Cir. 2004).

23. Véase Reidenberg, Joel R., «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, vol. 153 (2005), pág. 1952.

24. Véase Goldsmith, Jack y Wu, Timothy, *Who Controls the Internet? Illusions of a Borderless World*, 2006, pág. 1, en donde se subraya esta tesis de manera amplia y detallada con relación a este asunto.

25. Véase Reimann, Mathias, «Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage», *Michigan Journal of International Law*, vol. 24 (2003), pág. 667-668.

26. Véase Dow Jones & Company Inc. v. Gutnick (2002) 210 *Commonwealth Law Reports* pág. 575, en http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html. El Tribunal Supremo de Australia ha afirmado su jurisdicción en un caso de difamación iniciado por un reclamante australiano contra Dow Jones & Co., sobre la base de un artículo publicado en Nueva Jersey pero accesible y descargado en Australia. No obstante, esta decision ha sido criticada, véase Kohl, Uta, «Defamation on the Internet-Nice Decision, Shame about the Reasoning: Dow Jones & Co. Inc. v. Gutnick», *International and Comparative Law Quarterly*, vol. 52 (2003), pág. 1049; Garnett, Nathan W., «Dow Jones & Co. v. Gutnick: Will Australia's Long Jurisdictional Reach Chill Internet Speech World-

este planteamiento, y refleja así una posición mayoritaria [27]. Las democracias alemana, francesa y australiana han elegido reglas para la libertad de expresión que son consistentes con los derechos humanos, pero que no reflejan la protección que ofrece la Primera Enmienda de la Constitución de los EE.UU. [28]

Más recientemente, ha surgido otro caso interesante en 2010 como es el asunto *Google-Italia* [29], aunque se sale del supuesto relativo a contenidos nocivos, ya que en él varios ejecutivos de esta empresa han sido condenados penalmente por infracción de las normas sobre protección de datos personales. Frente a la posición de Google, que considera que no está sometida más que al derecho de EEUU, el tribunal italiano entendió que los ejecutivos de *Google Italia*, establecida y sometida al derecho italiano, eran responsables de la vulneración de la privacidad cometida al permitir la difusión de un video en donde se puede ver cómo unos adolescentes en Italia ejercen violencia física y moral frente a un niño que es autista, lo que supone una violación de su intimidad, en concreto, de los datos personales relativos a su estado de salud. Ciertamente, es probable que el juez italiano en este asunto fuera más allá de lo que exigía el Derecho de la UE en materia de protección de datos, ya que sólo habría responsabilidad si el provee-

---

Wide?», *Pacific Rim Law & Policy Journal*, vol. 13 (2004), pág. 61; Bone, Shawn A., «Private Hares in the Cyber- World: The Conundrum of Choice of Law for Defamation Posed by Gutnick v. Dow Jones & Co», *Washington & Lee Law Review*, vol. 62 (2005), pág. 279.

27. Véase J. Zittrain, «Be Careful What You Ask For: Reconciling a Global Internet and Local Law», en Thierer, Adam y Crews, Clyde Wayne Jr. (eds), *Who Rules the Net?*, 2003, pág. 19.

28. Véase la Declaración de Principios de la CMSI, apartado 5, que subraya, teniendo en cuenta el art. 29 de la Declaración Universal de los Derechos Humanos, que en el ejercicio de sus derechos y libertades «toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática».

29. Véase Sentenza n. 1972/2010, Tribunale Ordinario di Milano in composizione monocratica, Sezione 4.ª Penale, en http://www.giurcost.org/casi_scelti/Google.pdf.

dor de servicios de almacenamiento de datos (como Google) ha sido informado de la infracción y no actúa para solucionarlo [30]. No obstante, este caso resulta de interés porque, frente a la posición de Google que pretende hacer valer que los servicios de internet son prestados por una compañía de EE.UU. no sometida a las leyes nacionales italianas, el juez italiano asume plenamente el principio de la jurisdicción nacional y condena finalmente a los ejecutivos de esta empresa.

Con relación a todos estos asuntos, se podría decir que la afirmación de la jurisdicción estatal va en contra de la libertad básica de expresión y la libertad de información en el ciberespacio. Sin embargo, como el prof. Lessig ha demostrado, el hecho de que Internet se haya desarrollado anteriormente como un espacio libre no dice nada a cerca de cómo debería ser [31]. Los diseños tecnológicos desarrollados por los ingenieros de software, la arquitectura de la web, ha conllevado una especie de opción ideológica o filosófica, que refleja en gran medida los valores expresados en la Primera Enmienda de EEUU. El software es así la ley aplicable, pero este tipo de *lex informática* [32] no tiene por qué conllevar implicaciones normativas para la solución de conflictos regulatorios. Internet es lo que hacemos de él, no hay nada esencialmente dado e inmutable. Por el contrario, la innovación tecnológica está facultando a los Estados soberanos a hacer valer sus normas relativas a la actividad desarrollada en Internet [33]. Las tecnologías de filtrado y geo-localización permiten determinar la ubicación, y las reivindicaciones de la ubicuidad de la información

30. Véase Sartor, Giovanni y Viola de Azevedo Cunha, Mario, «The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents», *International Journal of Law and Information Technology*, vol. 18 (2010), pág. 369-371.

31. Véase Lessig, Lawrence, *Code and Other Laws of Cyberspace, op. cit.*, pág. 207-208.

32. Véase Reidenberg, Joel R., «Lex Informatica: The Formulation of Information Policy Rules through Technology», *Texas Law Review*, vol. 76 (1998), pág. 553.

33. Véase Reidenberg, Joel R., «Technology and Internet Jurisdiction», *loc. cit.*, pág. 1960.

en la web no se pueden sostener por más tiempo [34]. El caso *Yahoo!* ha terminado desplazando el poder de regular desde los tecnólogos de nuevo hacia los representantes políticos [35].

Dicho con otras palabras, las cuestiones sobre la extraterritorialidad y el ejercicio de jurisdicción en el ciberespacio han sido el foco de un intenso debate, y la dicotomía entre la libertad de expresión y la protección contra contenidos nocivos simplemente ha sido el tema articulador de este conflicto, a pesar de la existencia de otros tipos de extraterritorialidad dentro de Internet, por ejemplo, cuando EE.UU. ha exigido el cumplimiento de sus normas de propiedad intelectual fuera de su territorio. Como el prof. Goldsmith ha mantenido, la superación de una estricta jurisdicción territorial y la consiguiente regulación extraterritorial dentro del ámbito de Internet se justifica sobre la base de que el ciberespacio no es funcionalmente diferente de las actividades transnacionales realizadas a través de otros medios. Cada Estado tiene el derecho de regular los actos extraterritoriales que puedan producir daños u otros efectos locales dentro de su jurisdicción nacional. Este tipo de enfoque es común en los sistemas jurídicos nacionales y es legítimo hasta que un Estado haya dado su conformidad a una regla de Derecho internacional que especifique lo contrario [36]. Por otro lado, la regulación extraterritorial en el ámbito de Internet es posible, aunque no necesita ser perfecta con el fin de ser eficaz. Además, las normas sobre conflicto de

34. Véase King, Kevin F., «Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies», *Albany Law Journal of Science and Technology*, vol. 21 (2011), pág. 61.

35. Como señala Watt, «there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it. Analysis of such a claim has shown that it reverses the proper relationship between law and technology. Technology being purely manmade, and thus subject to ideological choice, should not dictate the way in which law manages conflicting interests arising through its medium», véase Watt, Horatia Muir, «Yahoo! Cyber-Collision of Cultures…», *loc. cit.*, pág. 695.

36. Véase Goldsmith, Jack L., «Against Cyberanarchy», *loc. cit.*, pág. 1239-1240.

leyes funcionan en el ámbito de Internet tanto como en otros campos de la vida real. Los asuntos antes mencionados (casos *CompuServe*, *Yahoo!*, *Gutnick* y *Google-Italia*) precisamente muestran que el Derecho Internacional está ayudando a resolver conflictos transnacionales de manera justa hasta que haya una solución basada en la armonización internacional [37].

No obstante, si en el ámbito de internet el ejercicio de la jurisdicción estrictamente territorial resulta injustificado porque dejaría muchos supuestos sin resolver en el Estado del foro, también es cierto que el ejercicio de la jurisdicción basada en los efectos (extraterritorial) puede conducir a un exceso de jurisdicción y a solapamientos. Algunos autores han propuesto fórmulas para sortear este problema [38]. Uno de estos criterios podría consistir en el ejercicio de la jurisdicción cuando se demuestre que las actividades de Internet se dirigen (target) de manera intencional hacia el territorio de un Estado. Se trataría de una versión más estricta de la ya referida doctrina de los efectos, y cuya aplicación necesitaría de la utilización de técnicas como la geo-localización o la zonificación, que no plantean problemas a día de hoy. Otra solución podría consistir en el uso del filtrado, que tiene dos vertientes, el filtrado desde el territorio del Estado de origen y el filtrado desde el territorio del Estado de destino. El segundo supuesto está más justificado, ya que permite que la riqueza de las redes [39] de Internet no disminuya de una forma drástica, como podría ocurrir en el primer caso si los suministradores de servicios de internet adoptaran una estrategia demasiado prudente evitan-

37. Véase Kightlinger, Mark F., «A Solution to the Yahoo! Problem? The EC Ecommerce Directive as a Model for International Cooperation on Internet Choice of Law», *Michigan Journal of International Law*, vol. 24 (2003), pág. 719, quien señala que la Directiva sobre comercio electrónico de la UE y sus reglas sobre el «country of origin» y el «home country control» serían un buen punto de partida para un acuerdo internacional sobre contenido en internet que simplificaría las controversias transnacionales.

38. Véase Schultz, Thomas, «Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Interface», *European Journal of International Law*, vol. 19 (2008), pág. 816.

39. Véase Benkler, Yochai, *The Wealth of Networks – How Social Production Transforms Markets and Freedoms* (2006).

do su exposición en numerosas jurisdicciones. El problema de ese segundo supuesto es que resulta contraproducente en el caso de los regímenes autoritarios, porque les facilita la restricción en el acceso a contenidos.

El consenso sobre la protección a la propiedad intelectual

Con la llegada de Internet, la protección de los derechos de propiedad intelectual fue cuestionada por las nuevas tecnologías y software (como el MP3 y Napster [40]) que permitían la distribución gratuita de la obras digitales de los tenedores de derechos de autor. Como se sabe, estas tecnologías han permitido a los usuarios de Internet descargar copias perfectas de canciones, películas y otras obras protegidas por las leyes nacionales y los tratados internacionales. Este problema sólo se ha agravado con la llegada de las tecnologías *peer-to-peer* (P2P) [41], un tipo de software que permite a los usuarios de Internet descargar archivos entre discos duros individuales sin que un servidor central tenga que hacer trabajo alguno [42]. Este tipo de tecnologías ha allanado el camino para la piratería masiva, con las consiguientes pérdidas para los autores y la industria en general. Las respuestas a esta nueva situación han sido de dos clases.

Por un lado, en EEUU (tras los primeros esfuerzos llevados a cabo por el Departamento de Comercio en 1995 con el objetivo de restaurar el «equilibrio» en el derecho de propiedad intelec-

40. Véase Dodes, Jeffrey L., «Beyond Napster, Beyond the United States: The Technological and International Legal Barriers to On-line Copyright Enforcement», *New York Law School Law Review*, vol. 46 (2002/2003), pág. 279.

41. Algunos autores han propuesto algunas soluciones a la cuestión, aún sin resolver, de las tecnologías P2P como alternativa al recurso a las reclamaciones judiciales frente a los usuarios o intermediarios, véase Lemley, Mark A. y Reese, R. Anthony «Reducing Digital Copyright Infringement Without Restricting Innovation», *Stanford Law Review*, vol. 56 (2004), pág. 1345; Litman, Jessica «Sharing and Stealing», *Hastings Communications and Entertainment Law Journal*, vol. 27 (2004), pág. 1; Weinstock Netanel, Neil «Impose a Noncommercial Use Levy to Allow Free Peer-To-Peer File Sharing», *Harvard Journal of Law & Technology*, vol. 17 (2003), pág. 1.

42. Véase Biegel, Stuart, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (2001), pág. 287.

tual [43]), la respuesta legal inmediata ha consistido en la adopción de nuevas leyes nacionales que han tratado de reforzar la protección tradicional otorgada por el régimen jurídico del derecho de autor. En EE.UU., la ley *No Electronic Theft Act* (NET Act) de 1997 y la *Digital Millenium Copyright Act* (DMCA) en 1998 se aprobaron con ese fin, aunque la DMCA ha sido acusada de inclinar la balanza a favor de las entidades privadas [44]. Del mismo modo, se adoptó en 2001 en la UE la Directiva sobre Derechos de Autor en la Sociedad de la Información con un fin similar [45]. Los tribunales nacionales también han hecho un gran esfuerzo para hacer frente a la cuestión de cómo proteger el copyright y en qué medida, a fin de no limitar excesivamente la información disponible en el dominio público, con un resultado que se inclina no obstante en favor de la protección de los derechos de autor [46].

Por otro lado, la respuesta (permitida por la legislación nacional) también ha sido técnica, porque la industria (subvencionada por el gobierno) ha utilizado la tecnología también para crear sistemas de gestión de derechos de autor llamados «sistemas de confianza», que es un software que hace que sea más fácil para los proveedores de información controlar el acceso y el uso de contenidos con copyright. De esta manera, la aplicación de la ley gracias al software es «*ex-ante*», libre del escrutinio legal y eficiente en un grado que no

43. Véase U.S. Department of Commerce, Task Force – Working Group on Intellectual Property Rights, «Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights», en http://www.uspto.gov/web/offices/com/doc/ipnii.

44. Véase Hughes, Justin, «The Internet and the Persistence of Law», *Boston College Law Review*, vol. 44 (2003), pág. 371.

45. Véase Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, *DO* L 167, de 22 de junio de 2001, pág. 10

46. Con relación a la jurisprudencia en EE.UU. puede citarse Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. 125 S. Ct. 2764 (2005); Eldred v. Ashcroft 537 U.S. 186 (2003); A & M Records, Inc. v. Napster, Inc. 114 F. Supp. 2d 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F. 3d 1004 (9th Cir. 2001); Universal City Studios, Inc. v. Corley 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom.*; Universal City Studios, Inc. v. Corley, 273 F 3d. 429 (2d Cir. 2001).

existe en el mundo no virtual [47]. Esta respuesta técnica, que sustituye al derecho público por el apoderamiento privado, ha merecido una crítica importante por parte de los autores especialistas, ya que este control perfecto llevado a cabo por empresas privadas de servicios de contenido de Internet puede tener consecuencias en relación con el derecho a la intimidad y la libertad de expresión, lo que a su vez genera otras cuestiones como las relacionadas con las doctrinas sobre «usos legítimos» y «dominio público» [48].

Los esfuerzos para dotarse de una regulación internacional en materia de propiedad intelectual han llevado a la conclusión de los Tratados de la Organización Mundial de la Propiedad Intelectual sobre Copyright, es decir, al Tratado de la OMPI sobre Derecho de Autor y al Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, de 1996. Se puede decir que estos acuerdos son el único ejemplo indiscutible del desarrollo de normas jurídicas sobre Internet con origen en el Derecho internacional de base convencional, al estilo *top-down*. Estos últimos tratados de la OMPI se han añadido a los tratados internacionales vigentes y de *larga data*, es decir, el Convenio de París para la Protección de la Propiedad Industrial y el Convenio de Berna para la Protección de las Obras Literarias y Artísticas (de 1883 y 1886, respectivamen-

47. Véase Elkin-Koren, Niva, «Copyright in Cyberspace: The Rule of the Law and the Rule of the Code», en Lederman, Eli y Shapira, Ron (eds.), *Law, Information and Information Technology*, 2001, pág. 135-136.

48. Véase, por ejemplo, Benkler, Yochai, «Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain», *New York University Law Review*, vol. 74 (1999), pág. 354; Cohen, Julie E., «A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace», *Connecticut Law Review*, vol. 28 (1996), pág. 981; id. «DRM and Privacy», *Berkeley Technology Law Journal*, vol. 18 (2003), pág. 575; Elkin-Koren, Niva «Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators», *Cardozo Arts & Entertainment Law Journal*, vol. 13 (1995), pág. 345; Lemley, Mark A. y Volokh, Eugene, «Freedom of Speech and Injunctions in Intellectual Property Cases», *Duke Law Journal*, vol. 48 (1999), pág. 147; Lessig, Lawrence, *The Future of Ideas*, 2001, pág. 4-16; Wenistock Netanel, Neil, «Locating Copyright Within the First Amendment Skein», *Stanford Law Review*, vol. 54 (2001), pág. 1; *Contra* Samuelson, Pamela, «Copyright and Freedom of Expression in Historical Perspective», *Journal of Intellectual Property Law*, vol. 10 (2003), pág. 319.

te), con el objetivo declarado de fortalecer la protección otorgada a los titulares de derechos de autor.

Hay una cierta controversia en cuanto a los resultados obtenidos por estos nuevos tratados. Mientras que para algunos no está del todo claro que estos tratados hayan desarrollado realmente la protección previamente existente [49], para otros los tratados de la OMPI pueden ser considerados como un resultado positivo, aunque la agenda de negociación súper-proteccionista de EE.UU. no haya tenido éxito [50]. También sería pertinente señalar aquí que la agenda de la UE en este sentido no era menos proteccionista [51]. Sin embargo, parece que la aplicación de estos tratados por las autoridades nacionales ha ido mucho más allá de lo que aquéllos exigen, y lo que exigen no es menos polémico (por ejemplo, en lo relativo a la adopción de normativa nacional para contrarrestar la elusión de medidas tecnológicas efectivas).

Por otra parte, el Acuerdo de la Organización Mundial del Comercio sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), que entró en vigor en 1995, ha sido un acuerdo internacional de referencia para la protección de los derechos de autor globalmente, y podría muy bien ser así en el ámbito de Internet. Este acuerdo no sólo establece normas y estándares de protección mínimos, y armoniza los procedimientos y recursos nacionales para la observancia de los derechos de propiedad intelectual, sino que, sobre todo, extiende el mecanismo de solución de diferencias de la OMC a este ámbito específico [52]. Esta extensión pretendía mejorar los mecanismos de control aplicables a las vulneraciones de derechos de autor que eran casi inexistentes

49. Véase Franda, Marcus, *Governing the Internet, The Emergence of an International Regime*, 2001, pág. 126, para quien estos recientes tratados de la OMPI son conservadores.

50. Véase Samuelson, Pamela, «The U.S. Digital Agenda at WIPO», *Virginia Journal of International Law*, vol. 37 (1997), pág. 435.

51. Véase Grewlich, Klaus W., *Governance in «Cyberspace», Access and Public Interest in Global Communications*, 1999, pág. 238 y 244.

52. Véase López Escudero, M., «Los derechos de propiedad intelectual en el comercio internacional», en Hinojosa Martínez, Luis y Roldán Barbero, Javier (eds.), *Derecho internacional económico*, (2010), pág. 163.

antes de la entrada en vigor del ADPIC. Los beneficios en el plano internacional de este tratado internacional se están sumando a otros beneficios a nivel nacional, es decir, algunos representantes de las industrias de derechos de autor ya han avanzado la idea de utilizar el Acuerdo sobre los ADPIC para poner en entredicho excepciones actuales a las leyes nacionales de copyright [53].

Pero este esfuerzo se ha visto intensificado con el Acuerdo Comercial de Lucha contra la Falsificación de 2010 (conocido como ACTA, en sus siglas en inglés). Este Acuerdo ha sido negociado casi en secreto por un grupo de Estados industrializados (EEUU, la UE, Japón, etc.), haciendo caso omiso del marco multilateral que procuran la OMPI o la OMC, con la intención de reforzar la observancia de las normas sobre propiedad intelectual, sobre todo en Internet [54]. Aunque entre los negociadores no se encuentran las grandes potencias emergentes fuente de la mayor parte de la piratería (China, India, Rusia, Brasil: los BRIC), la intención de sus promotores es la de generar unos estándares internacionales más elevados que se terminen imponiendo a los demás Estados de la Comunidad Internacional [55]. Entre los preceptos más polémicos de este ACTA se encuentran las disposiciones sobre criminalización de las infracciones a la propiedad intelectual [56], las medidas en frontera (que pueden dar paso a auténticas barreras al comercio internacional [57]) y, en particular, las medidas restrictivas a

53. Véase Samuelson, Pamela, «Copyright and Freedom of Expression in Historical Perspective», *loc. cit.*, pág. 332.

54. Véase Weatherall, Kimberlee, «Politics, Compromise, Text and the Failures of the Anti-Counterfeiting Trade Agreement», *Sydney Law Review*, vol. 33, (2011), pág. 230.

55. Véase Yu, Peter K., «Six Secret (and Now Open) Fears about ACTA», *SMU Law Review*, vol. 64, (2011), pág. 1035.

56. Véase Geiger, Christophe, «The Anti-Counterfeiting Trade Agreement and Criminal Enforcement of Intellectual Property: What Consequences for the European Union», *Max Planck Institute for Intellectual Property and Competition Law Research Paper núm. 12-04*, 2012, en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038272&rec=1&srcabs=2027920.

57. Véase Grosse Ruse-Khan, Henning, «A Trade Agreement Creating Barriers to International Trade?: ACTA Border Measures and Goods in Transit», *American University International Law Review*, vol. 26, (2011), pág. 645.

imponer en el ámbito digital. Entre estas medidas, cabe destacar las relativas a la vigilancia y control del contenido de los usuarios de Internet (con los problemas de privacidad y protección de datos que ello genera [58]) y las políticas de desconexión que se incentivan. Aunque las medidas como la desconexión al «tercer aviso» al estilo de la Ley HADOPI francesa [59] no se imponen, lo cierto es que se promueven por el ACTA medidas similares [60]. De momento, la UE ha firmado pero no ha ratificado este ACTA debido al rechazo del PE [61].

Como se puede observar, el Derecho Internacional ha tenido y probablemente seguirá teniendo un papel muy importante en la protección de los derechos de propiedad intelectual en el ámbito de Internet. No se trata sólo de que hay una cierta regulación en este campo, sino que además esta regulación es de la mejor clase. Tratados y Acuerdos internacionales, es decir, el «*hard-law*» en lugar del «*soft-law*», se usa aquí por los Estados para cooperar y establecer normas mínimas, exigir el establecimiento de mecanismos de aplicación nacionales, e imponer un sistema para resolver las controversias internacionales que surjan en este contexto. ¿Por qué razón nos encontramos con este enfoque tan consistente aquí, pero solo aquí? [62]

58. Véase Cerda Silva, Alberto J., «Enforcing Intellectual Property Rights by Diminishing Privacy: How the Anti-counterfeiting Trade Agreement Jeopardizes the Right to Privacy», *American University International Law Review*, vol. 26, (2011), pág. 601.

59. Véase Lucchi, Nicola, «Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI)», *Max Planck Institute for Intellectual Property and Competition Law Research Paper Series Núm. 11-07*, pág. 1, en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1816287.

60. Véase Bridy, Annemarie, «ACTA and the Specter of Graduated Response», *American University International Law Review*, vol. 26, (2011), pág. 559.

61. Véase Segura Serrano, Antonio, «El Acuerdo comercial de lucha contra la falsificación (ACTA): una evaluación desde el Derecho de la UE», *Revista General de Derecho Europeo*, núm. 28, (2012), pág. 1, en www.iustel.es.

62. Es cierto que la persecución del crimen en el ciberespacio ha conducido a la conclusión de otro tratado internacional, el Convenio sobre la Ciberdelincuencia de 2001, en el marco del Consejo de Europa. Sin embargo, el esfuerzo desplegado para alcanzar y aplicar los objetivos de este tratado no ha sido tan

La convergencia de intereses entre los Estados nacionales y los titulares de derechos de autor con grandes activos en propiedad intelectual ha hecho que sea posible para el Derecho Internacional desempeñar un papel importante en la regulación de este ámbito específico de Internet. Así que parece que sólo si el Derecho Internacional cumple completamente las expectativas de negocio en el ámbito de Internet será la herramienta preferida de los Estados para regular este ámbito de actividad humana.

En este sentido, parece bastante difícil de implementar una de las líneas de acción de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) auspiciada por las Naciones Unidas y la UIT (Ginebra y Túnez), que prevé «el desarrollo y promoción de la información en el dominio público, como un importante instrumento internacional que promueve el acceso de todos a la información» [63]. La pregunta sigue siendo si la ONU llegará a ser alguna vez una estructura internacional tan efectiva como, por ejemplo, la OMC, para tratar de regular este ámbito de la actividad humana y para implementar esa regulación.

DIFERENTES ENFOQUES RESPECTO DE LA CUESTIÓN DE LA PRIVACIDAD

El procesamiento a gran escala de datos personales estaba reservado inicialmente a las instituciones con bases de datos cen-

---

enérgico, véase, por ejemplo, Marler, Sara L., «The Convention on Cybercrime: Should the United States Ratify?», *New England Law Review*, vol. 37 (2002), pág. 183; Hopkins, Shannon L., «Cybercrime Convention: A Positive Beginning to a Long Road Ahead», *Journal of High Technology Law*, vol. 2 (2003), pág. 101; Weber, Amalie M., «The Council of Europe's Convention on Cybercrime», *Berkeley Technology Law Journal*, vol. 18 (2003), pág. 425.

63. Cumbre Mundial sobre la Sociedad de la Información, *Plan de Acción*, Ginebra, 12 de diciembre de 2003, Documento WSIS-03/GENEVA/5-S, de 12 de mayo de 2004, párrafo 10.3. El Plan de Acción establece que las líneas de acción persiguen «alcanzar los objetivos de desarrollo acordados a nivel internacional, con inclusión de los consignados en la Declaración del Milenio, el Consenso de Monterrey y la Declaración y el Plan de Aplicación de Johannesburgo, mediante el fomento del uso de productos, redes, servicios y aplicaciones basados en las tecnologías de la información y las comunicaciones (TIC), y para ayudar a los países a superar la brecha digital», *ibid.*, párrafo 1.

tralizadas. La llegada del PC y de Internet cambiaron esa situación, y ahora hay muchos más participantes en la actividad del uso de la información personal. Casi cualquier persona con un ordenador y acceso a Internet puede recopilar y procesar información personal, lo que ha conducido a un cambio radical con respecto al tema de la privacidad [64]. Desde hace algún tiempo, los expertos en privacidad se han venido centrando especialmente en las actividades de creación de perfiles y extracción de datos por parte de las empresas de marketing [65]. Por lo tanto, la cuestión de la protección de los datos personales y la privacidad en la era de Internet se ha convertido en una preocupación fundamental de política pública [66], y los Estados se han dado cuenta de la importancia que tiene este problema en sí mismo para la democracia [67], por no hablar de su papel en el fomento del comercio electrónico. La Cumbre Mundial sobre la Sociedad de la Información ha recordado también lo importante que es este tema para el desarrollo de Internet [68].

64. Véase Schauer, Frederick, «Internet Privacy and the Public-Private Distinction», *Jurimetrics: The Journal of Law, Science, and Technology*, vol. 38 (1998), pág. 557-561.

65. Véase, por ejemplo, Kang, Jerry, «Information Privacy in Cyberspace Transactions», *Stanford Law Review*, vol. 50 (1998), pág. 1238-1241; Reidenberg, Joel R., «Setting Standards for Fair Information Practice in the U.S. Private Sector», *Iowa Law Review*, vol. 80 (1995), pág. 530.

66. Véase Gellman, Robert «Conflict and Overlap in Privacy Regulation: National, International, and Private», en Kahin, Brian y Nesson, Charles (eds), *Borders in Cyberspace, Information Policy and the Global Information Infrastructure*, 1997, pág. 255; Reidenberg, Joel R. y Gamet-Pol, Francoise, «The Fundamental Role of Privacy and Confidence in the Network», *Wake Forest Law Review*, vol. 30 (1995), pág. 106.

67. Véase Schwartz, Paul M., «Privacy and Participation: Personal Information and Public Sector Regulation in the United States», *Iowa Law Review*, vol. 80 (1995), pág. 557.

68. Véase Cumbre Mundial sobre la Sociedad de la Información, *Declaración de Principios, cit.*, cuyo principio núm. 5 establece que «[e]l fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC […] es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio».

La protección de la información personal no es la misma en todos los países, sino que varía bastante entre los diferentes Estados, y esta disparidad es notable cuando se comparan los enfoques adoptados por EE.UU. y la UE [69]. Aunque EE.UU. fue probablemente el primer país que reguló la privacidad, la protección que ha otorgado a la información personal siempre se ha basado en una política dominada por el mercado [70], junto a la fuerte influencia de los principios de la Primera Enmienda que favorecen el libre flujo de información [71]. Dentro de este modelo, el papel del Estado es limitado: las normas jurídicas y los derechos reconocidos tienen por objeto proteger sectores muy definidos, de modo que la privacidad se debe lograr principalmente a través de la autorregulación del sector y los códigos de conducta.

Esta situación ha sido muy criticada por algunos especialistas [72] que han identificado en la regulación internacional y, sobre todo, la regulación europea, una fórmula a seguir. Schwartz y Reidenberg han repetido insistentemente que el enfoque europeo, a diferencia del de EE.UU., es el más apropiado con respecto a la privacidad, porque con razón considera la protección de datos como un asunto de derechos civiles [73]. Estos autores han puesto de relieve la función normativa del derecho a la intimidad en la gobernabilidad democrática, y sostienen que un modelo basado en la autorregulación y el mercado puede tener efectos dañinos para la democracia deliberativa [74]. Sin embargo, la cultura de la

69. Véase Reidenberg, Joel R. «Resolving Conflicting International Data Privacy Rules in Cyberspace», *Stanford Law Review*, vol. 52 (2000), pág. 1319.

70. *Ibid.*, pág. 1318; véase también Samuelson, Pamela, «A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy», *California Law Review*, vol. 87 (1999), pág. 770-773.

71. Véase Swire, Peter P. y Litan, Robert E., *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, 1998, pág. 153.

72. Véase Reidenberg, Joel R., «Restoring Americans' Privacy in Electronic Commerce», *Berkeley Technology Law Journal*, vol. 14 (1999), pág. 771.

73. Véase Schwartz, Paul M. y Reidenberg, Joel R., *Data Privacy Law: A Study of United States Data Protection*, 1996, pág. 39-42.

74. Véase Schwartz, Paul M., «Privacy and Democracy in Cyberspace», *Vanderbilt Law Review*, vol. 52 (1999), pág. 1615, quien considera que ninguna otra opción más que la imposición de estándares a través de la ley conseguirá el objetivo de

información en EEUU puede estar cambiando. En cierta medida, existe una preocupación creciente entre la población estadounidense con relación al amplio uso de tecnologías de la información para construir perfiles de individuos. Esta preocupación explica por qué la Comisión Federal de Comercio (FTC) y el Congreso de los EE.UU. han tratado de mejorar los derechos sustantivos y procesales de los individuos con respecto a su derecho a la privacidad [75], si bien es cierto que esta regulación es aún limitada por su enfoque sectorial [76].

El otro enfoque predominante, el enfoque europeo (que es también el modelo que existe en países como Canadá, Australia, Nueva Zelanda y Hong Kong [77]), se ha construido a través de una norma de protección de datos omnicomprensiva [78]. En este modelo, hay un régimen jurídico general que otorga un amplio conjunto de derechos y obligaciones para el tratamiento de los datos personales y, por contraposición a lo que sería una política cimentada en el mercado, se basa en una perspectiva de derechos humanos donde los usuarios no son «consumidores» sino «ciudadanos».

---

desarrollar normas efectivas sobre privacidad; id., «Internet Privacy and the State», *Connecticut Law Review*, vol. 32 (2000), pág. 815, en donde analiza los fallos en la retórica dominante que favorece el mercado, la regulación de abajo hacia arriba y la autoregulación de la industria; Cohen, Julie E., «Examined Lives: Informational Privacy and the Subject as Object», *Stanford Law Review*, vol. 52 (2000), pág. 1373, quien argumenta que tanto las medidas legales como las tecnológicas reforzarán la protección de la privacidad de los datos.

75. Véase Cate, Fred H., «Privacy Protection and the Quest for Information Control», en Thierer, Adam y Crews, Clyde Wayne Jr. (eds.), *Who Rules the Net?*, 2003, pág. 311.

76. Véase Solove, Daniel J., *The Digital Person, Technology and Privacy in the Information Age*, 2004, pág. 67; Zimmerman, Rachel K., «The Way the 'Cookies' Crumble: Internet Privacy and Data Protection in the Twenty-first Century», *New York University Journal of Legislation and Public Policy*, vol. 4 (2001), pág. 452-453.

77. Véase Givens, Beth, «Privacy Expectations in a High Tech World», *Santa Clara Computer and High Technology Law Journal*, vol. 16 (2000), pág. 348.

78. Véase Schwartz, Paul M., «European Data Protection Law and Restrictions on International Data Flows», *Iowa Law Review*, vol. 80 (1995), pág. 471, que hace un análisis del contenido de los estándares materiales europeos.

Como resultado de ser parte en el Convenio Europeo de Derechos Humanos (CEDH) y otros acuerdos internacionales, los países europeos tienen ciertas obligaciones, tales como asegurar el respeto a la vida privada y familiar, del domicilio y de la correspondencia (art. 8 CEDH). En concreto, en el contexto digital, existen varios textos jurídicos internacionales relativos a la protección de la privacidad y de los datos que tienen un origen o resabio europeo innegable. Dentro de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), las Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980 han sido seguidas por la Declaración Ministerial de Ottawa sobre la Protección de la Privacidad en las Redes Globales celebrada en 1998 [79]. Esta última reafirma los objetivos establecidos en las Directrices de privacidad de 1980 y el «compromiso relativo a la protección de la intimidad en las redes globales, con el fin de garantizar el respeto de derechos importantes», y ambos textos vienen a establecer lo que se ha llamado como «principios tecnológicos neutrales» para la protección de los datos personales en el ámbito internacional.

La OCDE, sin embargo, sigue haciendo hincapié en las repercusiones económicas de la protección de datos, es decir, se centra en los individuos como «usuarios» y «consumidores» en lugar de tratarlos como «ciudadanos». Un enfoque ligeramente diferente puede encontrarse en el Consejo de Europa en la que se han adoptado dos importantes textos jurídicos: la Convención de 1980 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y las Directrices de 1999 para la protección de las personas respecto a la recogida y tratamiento de datos personales en las autopistas de la información [80].

79. OCDE, Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, en http://www.oecd.org/internet/interneteconomy/15590267.pdf; OCDE, Declaración Ministerial relativa a la protección de la intimidad en las redes globales, Ottawa, 7-9 de octubre de 1998, en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/C.10-cp–Declaraci-oo-n-ministerial-Ottawa.pdf.

80. Consejo de Europa, Recomendación núm. R(99)5 del Comité de Ministros de los Estados Miembros sobre la protección de la intimidad en in-

Por último, la Directiva de la UE de 1995 sobre la protección de datos personales [81] es «la iniciativa mundial sobre privacidad de datos más ambiciosa y de mayor alcance de la era de la alta tecnología» [82]. Una característica distintiva de esta norma es su efecto extraterritorial, logrado a través de la prohibición del artículo 25, que impide la transferencia de datos a Estados que no ofrecen «un nivel adecuado de protección» de la información personal. Esta prohibición se convirtió claramente en una amenaza para los flujos de datos procedentes de la UE hacia EE.UU., ya que los funcionarios europeos han considerado que la legislación de EE.UU. no es lo suficientemente protectora de los datos personales [83]. Con esta Directiva sobre protección de datos, la UE ha establecido el estándar internacional y la agenda en este campo para muchos años.

Una especie de entendimiento entre los EE.UU. y la UE era necesario con el fin de evitar la interrupción de los flujos

---

ternet, Directrices para la protección de las personas respecto a la recogida y tratamiento de datos personales en las «autopistas de la información», de 23 de febrero de 1999, en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/recomendaciones/common/pdfs/Recomendacion_99_5_Internet.PDF.

81. Véase Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *DO* L 281, de 23 de noviembre de 1995, pág. 31; parcialmente reemplazada por la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), *DO* L 201, de 31 de julio de 2002, pág. 37.

82. Véase Salbu, Steven R., «The European Union Data Privacy Directive and International Relations», *Vanderbilt Journal of Transnational Law*, vol. 35 (2002), pág. 655; véase también Fromholz, Julia M., «The European Union Data Privacy Directive», *Berkeley Technology Law Journal*, vol. 15 (2000), pág. 461.

83. Véase Shaffer, Gregory, «Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards», *Yale Journal of International Law*, vol. 25 (2000), pág. 50-51, quien afirma que esta prohibición hubiera prevalecido en el caso de que EE.UU. hubiera decidido iniciar una disputa en el marco del sistema de solución de controversias de la OMC bajo el GATS.

de datos, y así es como el mayor esfuerzo de cooperación internacional hasta la fecha con efectos reales en este área se ha logrado mediante un acuerdo de «Puerto Seguro» entre EE.UU. y la UE [84]. Dado que la Directiva de la UE sobre la protección de datos entró en vigor en 1998 y la prohibición de transferencia de datos era de aplicación inmediata, el Departamento de Comercio de EEUU y la Comisión Europea trataron de llegar a algún tipo de entendimiento común en materia de protección de datos. La propuesta de EE.UU. para un Acuerdo de Puerto Seguro fue aceptada finalmente, después de dos años de negociaciones, por la Comisión Europea en julio de 2000. Este Acuerdo de Puerto Seguro establece los principios básicos de privacidad de datos a seguir por la industria.

Las empresas que se unieran a los principios de puerto seguro para la protección de la privacidad serían colocadas por el Departamento de Comercio en la lista de su página web de empresas certificadas y, a la inversa, la UE y su Estados miembros no las impugnarían o condicionarían de alguna otra manera las transferencias de datos hacia ellas [85]. Algunos especialistas han evaluado este acuerdo como un compromiso institucional para preservar el flujo libre de información salvaguardando las preocupaciones europeas [86]. Sin embargo, otros consideran este Acuerdo de Puerto Seguro como insuficiente [87] o incluso como un acto de rendición

84. Véase Decisión de la Comisión 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, *DO* L 215, de 25 de agosto de 2000, pág. 7.

85. Véase US Department of Commerce, *Safe Harbor*, en www.export.gov/safeharbor.

86. Véase Shaffer, Gregory, «Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements», *Columbia Journal of European Law*, vol. 9 (2002), pág. 58.

87. Véase J.M. Wakana, «The Future of Online Privacy: A Proposal for International Legislation», *Loyola of Los Angeles International and Comparative Law Review*, vol. 26 (2003), pág. 168 y 176.

por parte de la UE [88], ya que se deja la protección de datos en manos de la industria privada y la autorregulación. No parece pues que este tipo de acuerdo que se ha negociado vaya a servir como una solución permanente a la disparidad de la protección de la privacidad entre EE.UU. y Europa.

De hecho, la UE ya ha manifestado su incomodidad con la escasa observancia de este Acuerdo por parte de las empresas de EEUU, y lo poco efectivos que son los mecanismos establecidos en el mismo para hacer frente a las infracciones de la protección de datos [89]. Un ejemplo reseñable es el caso de *Google-DoubleClick*: cuando *Google* compró *DoubleClick*, empezó a acumular masivamente, sin consentimiento expreso, datos sobre perfiles de usuarios individuales de su motor de búsqueda hasta un máximo de dos años completos, con el objeto de poder realizar una publicidad más ajustada a esos perfiles. El Grupo de Trabajo del art. 29 de la Directiva sobre Protección de Datos contactó con Google solicitando colaboración y un mayor respeto de la normativa europea sobre protección de datos personales, pero sin mucho éxito [90].

Pero hay otra consideración que hacer desde la perspectiva del Derecho internacional. El acuerdo de «Puerto Seguro» claramente no es un Tratado internacional. No se ha firmado ni ratificado por las partes, por lo que no está sujeto a la Convención de Viena de 1969 sobre el Derecho de los Tratados. A lo sumo,

88. Véase Reidenberg, Joel R., «E-Commerce and Trans-Atlantic Privacy», *Houston Law Review*, vol. 38 (2001), pág. 744; Salbu, Steven R., «The European Union Data Privacy Directive and International Relations», *Vanderbilt Journal of Transnational Law*, vol. 33 (2000), pág. 681.

89. Véase Leather, Daniel R., «Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement», *Case Western Reserve Journal of International Law*, vol. 41 (2009), pág. 193.

90. Véase Article 29 Data Protection Working Party, *Press Release on Google's reply to the Opinion on data protection issues related to search engines*, de 16 de septiembre de 2008, en http://ec.europa.eu/justice/policies/privacy/news/docs/pr_16_09_08_en.pdf; véase también Article 29 Data Protection Working Party, *Press Release: EU data protection group says Google, Microsoft and Yahoo! do not comply with data protection rules*, de 26 de mayo de 2010, en http://ec.europa.eu/justice/policies/privacy/news/docs/pr_26_05_10_en.pdf.

se podría sostener que se trata de un «acuerdo de caballeros» o un acuerdo político. No obstante, algunos autores lo consideran como un supuesto de los nuevos tipos de regulación internacional [91]. Este acuerdo de Puerto Seguro sería un ejemplo de instrumento de «*soft-law*», en contraposición con el «*hard-law*», aunque en cuanto a sus efectos puede muy bien lograr una armonización de facto de la protección de la privacidad de datos (aunque sea a la baja).

Pues bien, en comparación con la protección de la propiedad intelectual ofrecida por el *hard-law*, es decir, a través de Tratados internacionales, de nuevo es llamativo que la regulación de Internet en este área del derecho a la protección de los datos personales sólo se ha podido alcanzar con un instrumento de *soft-law*. Sin embargo, no es tan sorprendente. Se necesita una cooperación internacional contundente en este campo, pero cuando los intereses empresariales dentro de EE.UU. están en juego [92], incluso existiendo apoyo de la población, es difícil que puedan conseguirse unos textos internacionales con más fuerza jurídica.

Conclusiones

Aunque intuitivamente pueda afirmarse la importancia que el Derecho internacional debe revestir en la regulación de Internet, debido a su carácter global, a través de este trabajo se ha intentado demostrar el rol que hasta hoy ha venido teniendo el ordenamiento internacional en la reglamentación de ciertos aspectos cruciales del ciberespacio. Del mismo modo, se ha puesto en evidencia que ese rol del Derecho internacional no es el mismo en los distintos apartados analizados. Mucho mayor en el ámbito de la protección de la propiedad intelectual, sin embargo es aún incipiente en lo que se refiere a la protección de la privacidad y el derecho a la intimidad. Como en tantas otras materias

91. Véase Perritt, Henry H. Jr., «The Internet is Changing the Public International Legal System», *Kentucky Law Journal*, vol. 88 (2000), pág. 940.

92. Véase Gellman, Robert «Conflict and Overlap in Privacy Regulation…», *loc. cit.*, pág. 274.

reguladas por el Derecho, son la voluntad política y los intereses económicos en juego los que explican la desigual capacidad de influencia que ejerce el ordenamiento internacional en los distintos aspectos antes examinados. Pero incluso, a falta de Derecho internacional convencional, y debido al efecto relativo de los tratados internacionales, que hace difícil avanzar en esta vertiente, se puede comprobar que el ejercicio de la jurisdicción estatal para los supuestos surgidos en el marco de Internet ha encontrado una solución jurídica conforme a las reglas tradicionales de este ordenamiento. Así, no puede hoy día sostenerse que Internet es un espacio libre y fuera del alcance de la autoridad estatal.

Sin llegar a proponer la creación de una organización internacional para la ordenación de la gestión de este importantísimo recurso que constituye en la actualidad Internet, sí que debe afirmarse el relevante rol que el futuro aguarda para el Derecho internacional en este ámbito. Como se ha avanzado, hay cuestiones aún por dilucidar, cualitativa y cuantitativamente hablando, como las relativas a la gobernanza de Internet, el uso de la fuerza en este entorno, la instauración de un derecho al acceso a Internet, etc., y no será sino el ordenamiento internacional el llamado a resolverlas con carácter global. Ese futuro nos aguarda a la vuelta de la esquina.

EL DERECHO DE INTERNET

Pablo García Mexiá*

Internet y el derecho: notas históricas

La irrupción masiva de Internet en las sociedades desarrolladas a partir de los inicios de los años noventa del siglo pasado ha venido generando en el mundo de las Ciencias Sociales en general, y en el del Derecho en especial, dos principales fases (u «olas») de respuesta.

La primera «ola»: El ciberespacio como «lugar» y la llamada ciberanarquía (hasta 1996 y esporádicamente desde entonces)

En febrero de 1996, justo un día después de que el entonces Presidente de los EE.UU. Bill Clinton promulgara la Telecommunications Decency Act de 1996, John P. Barlow, co-fundador de una de las más activas entidades de cibernautas pioneros, la Electronic Frontier Foundation, decidía enfrentarse a ese texto «colgando» en la Red la que llamó «Declaración de Independencia del Ciberespacio». Estos son algunos breves extractos especialmente expresivos de la «Declaración»:

> [En el Ciberespacio] no tenemos gobierno electo, ni es probable que lo tengamos, de ahí que me dirija a ustedes [Gobiernos del Mundo Industrializado] con no mayor autoridad que aquélla con la que habla la propia libertad. Yo declaro que el espacio social global que estamos construyendo es por naturaleza independiente de las tiranías que ustedes pretenden imponernos. Ustedes no tienen

* Pablo García Mexiá, es Profesor de Derecho de Internet en The College of William & Mary (Virginia, Estados Unidos) y Letrado de las Cortes.

> ningún derecho moral para gobernarnos, ni poseen método alguno de coerción que debamos temer con fundamento. Los gobiernos obtienen sus justos poderes del consentimiento de los gobernados. Ustedes no han solicitado ni recibido el nuestro. [...] Sus conceptos jurídicos de propiedad, libertad de expresión, derecho a la identidad, libertad de circulación, y contexto no nos son aplicables. Se basan en la materia. Aquí [en el Ciberespacio] no hay materia.

La alta significación de este texto reside en que supo materializar, apoyándose en la mejor tradición constitucional norteamericana, la más profunda idiosincrasia de los fundadores de la Red, y de sus primeros «exploradores». Ha de recordarse que, sin perjuicio de algunos desarrollos europeos, es fundamentalmente en los EE.UU. donde nace la Red. Y EE.UU., también es sabido, es el país del Thomas Jefferson que redacta la Declaración de Independencia, el del pactismo municipal tan hondamente arraigado en la libertad personal, el del «Destino Manifiesto» que no admite fronteras. Personajes como Barlow encajan casi a la perfección en este contexto.

No obstante, y además de por lo dicho, las palabras de Barlow tienen una gran importancia al constituir el mejor símbolo de la concepción social ciberlibertaria, para la que el ciberespacio es diferente del «aquí», razón por la cual debe disfrutar de cierta autonomía frente a los soberanos del mundo físico, o «espacio de carne», en su gráfica y hasta cierto punto agresiva terminología [1]. A fin de cuentas, para los defensores de esta concepción, Internet sería un espacio ajeno al Derecho, inmune a él, un espacio sin ley. Una cosa es desde luego bien clara: Internet es un espacio nuevo, y como tal, un ámbito donde el Derecho está empezando a llegar.

El primer internauta fue además:

> —Un tipo humano especialmente indómito. Joven (muy joven incluso, pues como resalta Negroponte [2], quizá la más importante «brecha digital» sea justamente la de la edad),

1. Véase Hunter, D., «Cyberspace as Place and the Tragedy of the Digital Anticommons», *California Law Review*, vol. 91 (2003), marzo, núm. 2.

2. Véase Negroponte, N., *Being Digital*, Nueva York: Alfred A. Knopf, 1995. Hay traducción española: *El mundo digital*, Barcelona: Ediciones B.

—con un nivel acomodado de ingresos económicos,
—de alta formación (ordinariamente técnica),
—que enlazaba fácilmente con los postulados de liberalismo extremado, lindantes con el anarquismo, de textos como el que nos servían para comenzar.

Bowrey [3] ha concretado que este «tipo humano», que propugna un ciberespacio libre de Derecho y libre de Estado, responde a las «relaciones personales y relativamente casuales de las comunidades de ingeniería californianas» de los primeros tiempos de Internet (década de los sesenta), a su vez marcadas por «su masculinidad y su *frikismo* tecnológico». Bien pronto, en un trabajo señero de 1996, Johnson y Post [4] trasladaban al ámbito científico estas tendencias sociales, y no dudaban en propugnar que la única estructura de poder en Internet fuera la que sus operadores protagonizan (autogobierno), siendo el único Derecho el que también éstos se puedan dar (autorregulación). Post ha reincidido en estas tesis en una excelente obra de 2009 [5]. Esa creencia en la inmunidad al Derecho y al poder del ciberespacio, tiene una explicación adicional: el carácter descentralizado de Internet, que algunos han llegado a emparentar con el federalismo [6].

Una relevante y lógica consecuencia de esa descentralización es además el hecho de que en el seno de la Red desaparece el concepto de frontera geográfica [7]. En el mundo «virtual», resulta intrascendente que un ordenador acceda a Internet o que vierta al ciberespacio determinados contenidos desde uno u otro punto del globo: desde cualquiera de ellos será accesible la informa-

3. Véase Bowrey, K., *Law and internet cultures*, Nueva York: Cambridge University Press, 2005, pág. 49.

4. Véase Johnson, D.R. & Post, D.G., «Law and Borders. The Rise of Law in Cyberspace», *Stanford Law Review* (1996), pág. 48.

5. Véase Post, D.G., *In Search of Jefferson´s Moose: Notes on the State of Cyberspace*, Oxford: Oxford University Press, 2009.

6. Véase Burk, D., «Federalism in Cyberspace», 28 *University of Connecticut Law Review* (1996), pág. 1095.

7. Véase Barnes Vázquez, J., «La internet y el derecho», en Chinchilla Martín, C. (dir.), *Ordenación de las telecomunicaciones*, Madrid: Consejo General del Poder Judicial, 1997.

ción, y desde cualquiera de ellos será transmisible; por lo tanto, también en cualquiera de tales puntos del planeta podrán surgir efectos jurídicamente relevantes.

La segunda «ola»: «No cabe inmunidad frente al Derecho» (desde 1996)

En cualquier caso, la visión ciberlibertaria no tardaría en hallar contestación, en lo que sería el inicio de un intensísimo debate entre los juristas especializados en Internet, fundamental, aunque no únicamente, de los EE.UU. Como precisa Hunter [8], esa contestación fue doble:

—Por un lado, se dirigió contra las bases descriptivas del escepticismo gubernamental y regulatorio;
—por otro, contra sus bases normativas.

Los ataques anti-ciberlibertarios

Fue Goldsmith [9] quien encabezó el inicio del ataque descriptivo, al sostener que el ciberespacio no constituye un lugar distinto del espacio real, en la medida en que las operaciones llevadas a cabo en aquél no difieren en modo alguno de las realizadas en éste. Esta tesis ha sido contundentemente preconizada en Europa por autores como los españoles Areilza y Mayor [10], si bien no a efectos puramente descriptivos (por seguir la terminología de Hunter), sino también normativos; es decir, con el propósito de defender la necesidad de regular la Red como cualquier otra faceta de la vida humana.

Por su parte, y de nuevo en los EE.UU., Netanel [11] abanderó el ataque normativo al mencionado escepticismo. Este autor confu-

8. Véase Hunter, D., «Cyberspace as Place…», *loc. cit.*, pág. 450.

9. Véase Goldsmith, J.L., «Against Cyberanarchy», 65 *University of Chicago Law Review* (1998), pág. 1199.

10. Véase De Areilza, J.M., «Una perspectiva europea sobre el gobierno de internet», en Mayor, P. y De Areilza, J.M. (eds.), *Internet, una profecía*, Barcelona: Ariel, 2002.

11. Véase Netanel, N.W., «Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory», *California Law Review* (2000), pág. 88.

taba el anclaje contractualista lockiano (recuérdense las alusiones al necesario «consentimiento de los gobernados») del más radical ciberlibertarismo, argumentando que es la propia democracia liberal la que exige la intervención estatal, a fin de asegurar su misma supervivencia.

La regulación jurídica de la Red es un hecho hoy en día

El problema no radica en absoluto en el hecho de si el ciberespacio es o no «un lugar». Recordemos que Internet puede ser contemplada y conceptuada desde múltiples perspectivas, no sólo la «espacial». De ahí que pretendamos, sin dejar por supuesto de edificar sobre ella, superar la controversia acerca de la Red como lugar. Lo que por ende ha de importar es calibrar si, no sólo entendida en clave de circunstancias espaciales o temporales, sino también como fenómeno de indeleble proyección política, social, económica, cultural o tecnológica, la Red puede y debe quedar sujeta al Estado y al Derecho.

Pues bien, Internet es un fruto del ingenio humano, es un fruto de su civilización. En esta medida, como tal fruto del ingenio y de la civilización humanas, el Derecho, se quiera o no, estará presente en la Red. No es posible ponerle «puertas al Derecho»: se colará indefectiblemente por la menor rendija que le abra la más insignificante relación humana, la más nimia relación social. Como, por otro lado, debe ser.

Ésta es asimismo la línea sostenida generalizadamente por la doctrina europea, donde las tesis ciberlibertarias no han tenido predicamento [12]. Más bien al contrario, como el propio Muñoz Machado [13] nos recuerda, no faltan quienes reclaman una urgente adaptación del poder del Estado a estas nuevas realidades y una inmediata intervención del Derecho. Por otra parte, tampoco se han producido

12. Véase Barnes Vázquez, J., «La internet y el derecho», *loc. cit.*; Frosini, F., «L'orizzonte giuridico dell'internet», *Il Diritto dell'informazione e dell'informatica*, año XVI, núm. 2, marzo-abril (2000); Zittrain, J.L., «The Generative Internet», *Harvard Law Review* (2006), vol. 119, núm. 7, mayo.

13. Véase Muñoz Machado, S., *La regulación de la red. Poder y derecho en internet*, Madrid: Taurus, 2000.

en Europa, desde parcelas ajenas al Derecho, manifestaciones tan extremadas como la de Barlow. Internet ha pasado «de la ilusión de ser una tierra de nadie, a la realidad de ser tierra de todos» [14].

No en vano, existen ya:
—Normas procedentes de organizaciones internacionales (el Consejo de Europa, por ejemplo);
—Normas emitidas por organismos supranacionales, como la Unión Europea;
—y normas emanadas por los distintos Estados, ya lo sean en este último caso por sus instituciones digamos «centrales», ya por entes territoriales como la región o el municipio.

Y todas esas normas disciplinan ya materias tan diversas como:

—La criminalidad
—Las telecomunicaciones
—O el comercio electrónico

Subraya al hilo de estas ideas Zittrain [15] que muchos Estados se han abstenido de regular la Red «en profundidad»; pero con ello no hace sino darnos a entender que la han regulado y la vienen regulando.

Los fundamentos del derecho de internet

La actual es una sociedad crecientemente basada en las tecnologías de la información y la comunicación (TICs). Éstas, como la Historia jurídica demuestra que ha sucedido con todos los demás sectores, generarán —están generando ya— particulares exigencias jurídicas. Tiene sentido pensar que esas exigencias se aglutinen en torno a una nueva rama del Derecho, propia de Internet como principal elemento impulsor de la sociedad de la información.

Acerca de la cuestión de si es más apropiado referirse a esta materia como «Derecho de las TICs», «Derecho del ciberespacio»

14. Véase Svantesoon, D.J.B., *Private International Law and the Internet*, Alphen aan den Rijn: Kluwer Law International, 2007, pág. 2.
15. Véase Zittrain, J.L., «The Generative Internet», *loc. cit.*

o «Derecho de Internet», Svantesson[16] defiende la idoneidad de la denominación «Derecho de Internet», notoriamente propugnada también en estas páginas (dada la excesiva amplitud de la primera —que incluiría temas estrictamente ajenos a Internet— y el carácter excesivamente literario de la segunda).

La propuesta de regulación que aquí se propone debe no obstante asentarse sobre dos fundamentos básicos.

El primero se refiere a sus fuentes, y a su vez se subdivide en dos: el no siempre fácil acomodo de posibles nuevas normas en materia de Internet en los respectivos acervos jurídicos nacionales e internacional; y el alcance que tal regulación deba tener, ya meramente estatal (o incluso de plano inferior), ya internacional, ya combinatorio de ambos.

El segundo es la constatación de que Internet posee de algún modo «una naturaleza», la cual, por lo que más adelante se explica, ha de respetarse por cualquier regulación: se trata de la apertura de la Red, a la que también se suele denominar su «neutralidad».

Dos aspectos sobre fuentes de esta rama del Derecho

Derecho nuevo frente a viejo Derecho

El primer aspecto sobre fuentes es la incidencia del Derecho de Internet sobre el acervo jurídico existente. La cuestión no fue históricamente pacífica, pues por ejemplo el Conseil d'État francés, en un Dictamen de 1998, señalaba que no era necesario crear un «Derecho de Internet» que, como rama jurídica nueva, pretendiera regular unificadamente este medio: bastaría una mera adaptación del Derecho ya vigente, en la medida exigida por Internet. También opinaban así Muñoz Machado [17] o, en los EE.UU., autores como Burk, Hardy ó Karl [18].

16. Véase Svanteesoon, D.I.B., *Private International Law...*, *loc. cit.*, pág. 22.

17. Véase Muñoz Machado, S., *La regulación de la red. Poder y derecho en internet, op. cit.*

18. Véase Burk, D., «Federalism in Cyberspace», *loc. cit.*; Hardy, I.T., «The Ancient Doctrine of Trespass to Web Sites», *Journal Online Law* (1996); Karl, D.J., «State Regulation of Anonymous internet Use after ACLU of Georgia and Miller», 30 *Arizona State Law Journal* (1998), pág. 513.

A mi juicio, ésta es cuestión más propia de los primeros tiempos de relación entre Internet y el Derecho, estando ya hoy prácticamente superada. Así, resulta indiscutible que, respecto de Internet y la sociedad de la información, debe aplicarse el Derecho general, el «viejo Derecho», igual que en cualquier otro ámbito social, dado que, aun cuando muchos de los problemas que en Internet se plantean son de nuevo tipo, también se dan en ella muchos viejos problemas, que admiten soluciones a través de las técnicas interpretativas tradicionales (como por ejemplo la analogía).

No obstante, es forzoso reconocer que, como hemos visto, Internet ha generado ya cotas nada despreciables de Derecho enteramente nuevo, uno de cuyos mejores ejemplos se encuentra sin duda en la regulación europea de los servicios de la sociedad de la información y del comercio electrónico. A mayor abundamiento, si esto ha sucedido en poco menos de veinte años, todo inclina a pensar que la tendencia a crear Derecho nuevo, específicamente aplicable a la Red, cuanto menos continuará —si no aumentará— en el futuro. Posiciones de alguna manera semejantes se han venido manteniendo por autores como Zittrain, en los EE.UU. [19]; y Pascuzzi, Reed ó Frosini, en Europa [20].

Derecho mundial frente a Derecho nacional

El ciberespacio constituye un excelente ejemplo de la actual insuficiencia de los Estados para resolver muchos problemas: en este sentido, Internet dista de poder ser regulada en exclusiva por los Estados [21]. Al fin y al cabo, como recuerda Pascuzzi [22], Internet es a la vez factor y producto de la globalización.

19. Véase Zittrain, J.L., «The Generative Internet», *loc. cit.*

20. Véase Pascuzzi, G., *Il diritto dell'era digitale: tecnologie informatiche e regole privatistiche*, Bologna: Il Mulino, 2006 ; Reed, Ch., *Internet Law: Text and Materials*, Cambridge-Nueva York: Cambridge University Press, 2004; Frosini, F., «L'orizzonte giuridico dell'internet», *loc. cit.*

21. Véase Villar Palasí, J.L., «Implicaciones jurídicas de internet», en *REDETI* núm. 5, 1999, junio.

22. Véase Pascuzzi, G., *Il diritto dell'era digitale…, op. cit.*

En efecto, al desbordar sus límites geográficos, para configurar un espacio virtual transfronterizo, la Red hace pequeño al Estado. Muchos autores estiman que la mayor parte de las regulaciones consideradas imprescindibles en Internet tendrá que hacerse a escala universal, mediante acuerdos entre los Estados, sin perjuicio de que éstos conserven el control sobre aspectos más locales de la Red [23].

Sin discrepar abiertamente de este punto de vista, sí conviene precisar que quizá no llegue a ser necesaria la universalidad para esa «mayor parte» de las regulaciones de Internet. O que sólo llegue a serlo pasado más tiempo del que en nuestros días se cree. Hoy por hoy estamos infinitamente lejos de haberla conseguido, pues resta multitud de regulaciones de importancia por llevarse a cabo a escala universal, y sin embargo Estados muy relevantes (así, los EE.UU.), e incluso la Unión Europea y sus Estados miembros, cuentan ya con un bagaje normativo muy amplio (ejemplo: en materia de comercio electrónico).

La naturaleza abierta o neutral de la Red

La Internet Engineering Task Force (IETF) es probablemente el organismo tecnológico por excelencia de Internet, de donde proceden sus líneas básicas de diseño. Uno de sus expresidentes, David Clark, manifestó en cierta ocasión que en IETF «se rechaza a los reyes, a los presidentes y las votaciones…»: más allá del respaldo del gobierno norteamericano, Internet iba surgiendo a golpe de avances tecnológicos, al margen de consideraciones políticas o jurídicas.

Esos avances tecnológicos eran a su vez fruto de una peculiar técnica de trabajo en el seno de IETF: los llamados RFCs o «Requests for Comments» (solicitudes de comentarios), ideados por Stephen Crocker. Las propuestas de nuevos estándares y protocolos, es decir, de nuevas pautas de funcionamiento de la Red, eran sometidas a la consideración de todos los demás miembros

23. Véase Muñoz Machado, S., *La regulación de la red. Poder y derecho en internet, op. cit.*; Villar Palasí, J.L., «Implicaciones jurídicas de internet», *loc. cit.*; Pascuzzi, G., *Il diritto dell'era digitale…, op. cit.*

de IETF (ingenieros y tecnólogos en general), «solicitando sus comentarios».

A partir de aquí, se activaban las dos reglas clave (no jurídicas, por supuesto, en cuanto que limitaban su ámbito a esa sola comunidad): la primera, «el consenso aproximado» («rough consensus») entre los distintos tecnólogos intervinientes en la discusión y posterior decisión: solo se creaba un nuevo estándar o protocolo de funcionamiento si el parecer general era favorable a ello. La segunda regla: el hecho de que el código simplemente «funcionase» en Internet («running code»), es decir, que, tras ser aprobado que ese nuevo estándar o protocolo pueda ser «subido a la Red», una vez en ella se desenvuelva sin problemas.

Internet saltaba pues a la sociedad a mediados de los noventa del pasado siglo como una red tecnológicamente preparada para albergar y transportar cualquier contenido. Y como una red socioculturalmente predispuesta a llevarlo a cabo. En una palabra, como una red abierta. O según el profesor Tim Wu prefirió denominarla en 2003, en expresión célebre desde entonces, como una red «neutral», en cuanto que «no favorece ninguna aplicación (o contenido) sobre otro» [24].

Esta red neutral o abierta se asentaba sobre una arquitectura tecnológica diseñada a semejanza de las redes neuronales y basada en la técnica denominada de «conmutación de paquetes», que eliminaba la necesidad de que la red en sí fuera «inteligente». Al contrario que con la técnica denominada de «conmutación de circuitos», mayoritariamente utilizada en las telecomunicaciones a lo largo del siglo XX (por excelencia, en la telefonía), y construida a partir de «redes muy inteligentes», la clave de la red Internet estaba en los extremos, en que la comunicación fluyera de «extremo a extremo» («end-to-end»). Como nos explica Post [25], una red «end-to-end» realiza «el número mínimo de tareas necesarias para trasladar mensajes de un sitio a otro»; este tipo de redes son pues «simples, al menos tan simples como los ingenieros consi-

24. Véase Wu, T., «Network Neutrality, Broadband Discrimination», *Journal of Telecommunications and High Technology Law*, vol. 2 (2003), pág. 141.

25. Véase Post, D.G., *In Search of Jefferson´s Moose…, op. cit.*

guen diseñarlas», pues apenas hacen «nada que no sea trasladar mensajes, todo lo demás se deja para las máquinas que operan en la periferia de la red». Según afirma el propio Post, Internet ha conectado «máquinas inteligentes a una red tonta». Esta fue, en fin, la base tecnológica sobre la que Vinton Cerf y Robert Kahn diseñaron el fundamental protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), en el año 1973.

En consecuencia, si su apertura es al fin y al cabo el principio esencial de Internet, en cuanto se halla en el núcleo de las razones de su éxito, toda regulación de Internet deberá en todo caso respetar su apertura, su neutralidad [26].

El contenido del derecho de internet

Internet no es un todo indiferenciado. Autores como Benkler [27] y Lessig [28], en los EE.UU. o Casanovas [29], en Europa, deslindan en su seno tres elementos principales:

—El estrato físico, constituido por la red: es decir, el complejo entramado de canalizaciones de toda índole (en ocasiones, el propio éter) que sirven de sustrato al código y los contenidos: por ejemplo las redes de cable, telefónicas o de fibra óptica, así como el espectro radioeléctrico.

—El estrato de los contenidos, evidentemente compuesto por las múltiples fuentes de información y conocimiento que Internet pone a disposición de sus usuarios en forma de servicios (gratuitos o de pago).

26. Véase García Mexía, P., *Historias de Internet. Casos y cosas de la Red de redes*, Valencia: Tirant Humanidades, 2012, págs. 41-67.

27. Véase Benkler, Y., «From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access», (2000) www.law.indiana.edu/fclj/pubs/v52/no3/benkler1.pdf; Benkler, Y., «Freedom in the Commons: Towards a Political Economy of Information», 52 *Duke Law Journal* (2003), pág. 1245.

28. Véase Lessig, L., *El código y otras leyes del ciberespacio*, Madrid: Taurus, 2001; Lessig, L., *The Future of Ideas: the Fate of the Commons in a Connected World*, Vintage, 2001.

29. Véase Casanovas Romeu, P., «Derecho, internet y Web semántica», en *Derecho a la intimidad y nuevas tecnologías*, Madrid: CGPJ, 2004.

—Y finalmente, el estrato lógico, plasmado en el llamado código, más concretamente, la conexión física y funcional entre ordenadores y redes de ordenadores, hecha posible por el software, los estándares de comunicación y los protocolos específicamente diseñados para ello. Sin la conexión generada por el software, los estándares de comunicación y los protocolos de Internet, ésta sencillamente no habría llegado a existir y no podría subsistir como tal.

La regulación de Internet no puede ser uniforme para todos y cada uno de estos tres estratos tecnológicos, debiendo por el contrario variar en función de cuál de ellos sea al que se dirija. La razón estriba en que estos tres estratos difieren esencialmente entre sí, sin perjuicio de converger a la hora de propiciar la misma existencia de Internet. Es decir, si bien es cierto que sin cualquiera de ellos Internet no puede siquiera operar, no lo es menos que como mínimo el soporte físico y los contenidos son perfectamente imaginables al margen de la Red.

En coherencia con todo lo afirmado, distinguiremos entre la regulación del soporte físico, la de los contenidos y la del código.

La regulación de la red física

La normativa de telecomunicaciones es la que en amplias regiones y múltiples países del mundo, y en todo caso por supuesto la Unión Europea, reglamenta este estrato de Internet.

Como resultado de los elementos condicionantes a los que seguidamente nos referiremos, la de telecomunicaciones es una regulación esencialmente imperativa para sus destinatarios. Tales elementos son sustancialmente tres:

—La garantía de la libre competencia, que pretende salvaguardar los mercados de las telecomunicaciones, y con los que los operadores de Internet deben necesariamente interactuar.

—La ordenación de recursos limitados, que es patente, a la vista de la creciente escasez del ancho de banda o del espectro radioeléctrico, como consecuencia de la expansión de usos altamente intensivos de Internet (para video o música, por ejemplo).

—Y la protección de los usuarios, especialmente si son finales y personas físicas, y aún con mayor motivo si, en este último supuesto, sufren algún tipo de desventaja social (una discapacidad, por ejemplo): éste es el objetivo de medidas generalizadas en la Unión Europea y otras regiones avanzadas del mundo, como el servicio universal de telecomunicaciones, la previsión de estatutos del usuario de servicios de telecomunicaciones, o la imposición a los operadores de determinadas obligaciones por razones de interés general (el acceso a un número telefónico de emergencias, a modo de muestra).

La regulación de los contenidos

La mayor o menor intensidad de la regulación en este ámbito de los contenidos de Internet está lógicamente en directa proporción al tipo de contenido de que se trate; de tal manera que contenidos delictivos en la Red requerirán obviamente la máxima intervención de los Estados y organizaciones internacionales. Otros contenidos, como los propios del comercio electrónico, es evidente que exigirán un margen de maniobra ajeno al poder del Estado y a normas imperativas, mucho mayor.

En este contexto ha de citarse la arraigada y amplia presencia que en el seno del ciberespacio ha tenido y tiene la autorregulación [30]. Ello se debe a esa «alergia» hacia el Derecho y hacia el poder que evidenciaban los primeros navegantes de la Red; y a la gran relevancia que la autorregulación tiene en general en la sociedad estadounidense, cuna principal de Internet.

La propia legislación de la Unión Europea ha consagrado la autorregulación, en forma de códigos de conducta voluntarios, al instar a los Estados miembros a impulsarla en el ámbito de los servicios de la información y del comercio electrónico y, en especial, a escala internacional y comunitaria. Estos códigos habrán

30. Véase Hunter, D., «Cyberspace as Place…», *loc. cit.*; Muñoz Machado, S., *La regulación de la red. Poder y derecho en internet, op. cit.*; Villar Palasí, J.L., «Implicaciones jurídicas de internet», *loc. cit.*; Barnes Vázquez, J., «La internet y el derecho», *loc. cit.*

de centrarse singularmente en la promoción de la salvaguardia de las normas sobre comercio electrónico incluidas en la Directiva 2000/31/CE, y la protección de los menores y de la dignidad humana, debiendo ser accesibles por vía electrónica (art. 16 Directiva 2000/31/CE).

Con todo ello en mente, la regulación de los contenidos de Internet se estructura en una triple dimensión:

—Dimensión política: la clave de la ordenación jurídico-política de estos contenidos es por supuesto la regulación de las libertades en Internet, destacando en este sentido la libertad de expresión, junto a derechos como la participación en asuntos públicos a través de herramientas como el voto electrónico, o los riesgos para los derechos al honor, intimidad y propia imagen y protección de datos que la Red ha venido a plantear.

—Dimensión penal: lamentablemente, el mundo del crimen se ha acomodado con asombrosa rapidez y eficacia al mundo digital, siendo notoria la existencia de toda una serie de nuevos delitos exclusivamente propios de Internet (el phishing, como ejemplo, por sólo citar uno); junto a versiones en red de tipos penales antiguos (la pederastia, entre otros).

—Dimensión económica: la regulación de los contenidos de Internet presenta en este sentido dos grandes frentes:

- El estudio de la repercusión de la Red en una de las áreas jurídicas sin duda más gravemente sacudidas por ella, la de la propiedad intelectual.
- Y el análisis del Derecho del comercio electrónico, manifestación jurídica de toda esa nueva y prometedora forma digital de hacer negocios, incluyendo en él sus dimensiones tributarias.

¿Regulación del código?

El elemento condicionante por excelencia de este tercer componente de Internet es la ya mencionada necesidad de preservar la apertura o neutralidad de la Red, a su vez clave del poderoso carácter innovador de Internet: recordemos en este sentido que

el código que dio origen a Internet no precisó de norma jurídica alguna para surgir y evolucionar tan satisfactoriamente como lo hizo.

Son de hecho esos factores los que explican la práctica inexistencia de cualquier tipo de regulación legal sobre el código de Internet en el mundo (con la salvedad de las matizaciones que seguidamente se expondrá). Todavía hoy sigue en este sentido siendo cierto que, como afirmara Lessig [31], «el código es el Derecho»: por concretarlo aún más, «los estándares de comunicación, el software y los protocolos» que animan la misma entraña del ciberespacio, todos ellos, y ninguna otra cosa, son «el Derecho».

Autores como Benkler [32] ó Lemley [33], junto a Post [34], Lessig [35] o Zittrain [36], han venido proclamando con insistencia que la Red habría de seguir «abierta» o «neutral». Por lo también entonces argumentado, nos sumamos a todos ellos desde estas páginas, con el importante respaldo adicional de la propia Unión Europea, cuya normativa sobre telecomunicaciones impone la garantía de las conexiones «extremo a extremo» como obligación para las autoridades en su caso competentes (arts. 8.3.b Directiva 2002/21/CE de 7 de marzo de 2002, sobre marco regulador común de redes y servicios, reforzada en esta misma línea por la Directiva 2009/140/CE de 25 de noviembre de 2009; y 12.1.g Directiva 2002/19/CE de 7 de marzo de 2002, relativa al acceso e interconexión).

No obstante, como anteriormente se afirmaba hay que hacer en este punto algunas matizaciones, que agruparemos bajo dos rúbricas, política una y tecnológica la otra.

31. Véase Lessig, L., *El código y otras leyes del ciberespacio, op. cit.*

32. Véase Benkler, Y., «From Consumers to Users…», *loc. cit.*

33. Véase Lemley, M.A., «Place and Cyberspace», *California Law Review*, vol. 91, (2003) marzo, núm. 2.

34. Véase Post, D.G., *In Search of Jefferson´s Moose…, op. cit.*

35. Véase Lessig, L., *El código y otras leyes del ciberespacio, op. cit.*; Lessig, L., *The Future of Ideas…, op. cit.*

36. Véase Zittrain, J.L., *The Future of the Internet and How to Stop it*, New Haven, Conn.: Yale U. Press, 2008.

Consideraciones políticas

Desde el ángulo político se atisban ya los intentos de una incipiente regulación, de la mano del gobierno de Internet, en particular del régimen de ICANN: una regulación cargada de polémica, y que a nuestro juicio deberá con justicia abrir paso a fórmulas de internacionalización, aunque sin olvidar la peculiar posición al respecto de los EE.UU. Esta indicación requiere ulteriores explicaciones, pues constituye el trasfondo de la referida polémica.

Efectivamente, hasta comienzos del siglo XXI, esos software, estándares y protocolos de comunicación que conforman la más consustancial de las dimensiones de Internet (la tecnológica), habían venido siendo gestionados por toda una serie de organismos de naturaleza enteramente privada, si bien relacionados con la Administración estadounidense. Como De Andrés Blasco [37] indica, los principales serían los siguientes:

—Organismos técnicos.

- ICCB (Internet Configuration Control Board, Junta de Control de la Configuración de Internet), encargado del seguimiento de la evolución técnica de los protocolos de comunicaciones;
- IAB (Internet Architecture Board, Junta para la Arquitectura de Internet), creada a partir de la ICCB, se ocupa del diseño, ingeniería y gestión de la Red, en especial del conjunto de protocolos TCP/IP;
- IETF (Internet Engineering Task Force, Grupo de Trabajo para la Ingeniería de Internet), en él ha delegado la IAB la responsabilidad del perfecto funcionamiento de la Red y la resolución de cuestiones relativas a la arquitectura y protocolos de comunicaciones;
- IRTF (Internet Research Task Force, Grupo de Trabajo para la Investigación sobre Internet), constituye la parte de investigación pura de la IAB;

37. Véase De Andrés Blasco, J., *Internet*, Madrid: Senado, 1999; De Andrés Blasco, J., «¿Qué es internet?», en García Mexía, P. (dir.), *Principios de derecho de internet*, Valencia: Tirant lo Blanch, 2005.

- ILTF (Internet Law Task Force, Grupo de Trabajo sobre el Derecho de Internet), de funciones obvias en el contexto de la propia IAB.

—Organismos de coordinación y representación. El esencial es sin duda ISOC (Internet Society, Sociedad de Internet), organización no gubernamental con fines de fomento de la utilización y desarrollo de la Red, dotada de la principal responsabilidad en cuanto a las grandes directrices y la administración de los recursos.

—Organismos de gestión de los nombres de dominio. El organismo de mayor relevancia es por supuesto ICANN (Internet Corporation for Assigned Names and Numbers), que, como consecuencia del control que los nombres de dominio permiten ejercer sobre el conjunto de la Red, ha venido a convertirse con el paso del tiempo en el órgano de gobierno y gestión de Internet por excelencia.

—Los nombres de dominio se organizan a través del llamado «sistema de nombres de dominio» (Domain Name System, DNS), gestionado por ICANN —sin perjuicio de la directa responsabilidad de las autoridades nacionales competentes, sobre sus correspondientes dominios de país abajo citados y sobre los propios dominios de segundo nivel—, y estructurado en torno a dos niveles:

- El nivel superior (Top Level Domains, TLDs), compuesto por otros tres grupos de dominios:
- Los llamados genéricos (gTLDs), en concreto, los siete originarios (.com, .edu, .gov, .org, .net, .mil, .int) y otros sucesivamente creados a partir de noviembre de 2000 (.biz, .info, .name, .coop, .aero, .pro, .museum, .travel, .post, .mobi, .jobs, etc.);
- y los de «código de país» (ccTLDs), por ejemplo: .eu (la Unión Europea, merced al Reglamento (CE) núm. 733/2002), .us (EE.UU., desde junio de 2002), .pt (Portugal), .ma (Marruecos), .jp (Japón), .au (Australia), etc.; a su vez susceptibles de presentar los llamados subniveles (sub-level TLDs), del tipo .com.arg (para una empresa argentina), .org.uk (para una ONG británica), .edu.cn (para una universidad china), etc.

- En junio de 2011 ICANN acordaba extender prácticamente al infinito el ámbito de los dominios de nivel superior (TLDs). La decisión hace posible la inclusión como tales de cualesquiera denominaciones, por ejemplo de empresas, de marcas comerciales, de sectores de actividad, de países, etc., del tipo: .repsol, .dieseleplus, .petróleos, o .portugal. Cierto que, con la idea de limitar, al menos de entrada, el alcance de la medida, no se admitirán solicitudes de personas individuales o físicas; además, las tasas de registro serán lo suficientemente elevadas como para disuadir del intento a la gran mayoría de empresas (y hasta a algún gobierno): nada menos que 185.000 $ (ICANN 2011).

—El segundo nivel es el que corresponde a la persona física o jurídica concretamente responsable de la página web de que se trate (ej.: la Unión Europea, en el dominio Europa, www.europa.eu).

Como antes indicábamos, este sistema constituye el trasfondo de la polémica. Ésta surge especialmente a propósito de ICANN, siendo el foro en el que se ha planteado la llamada Cumbre mundial sobre la sociedad de la información, celebrada en dos fases, bajo la égida de las Naciones Unidas y de la Unión Internacional de Telecomunicaciones.

La controversia está sintéticamente basada en:

—La pretensión de determinados países emergentes (China, Rusia y Brasil en particular) de participar de un modo más activo como Estados en el gobierno de Internet, a través de fórmulas de gestión que implicaran a las Naciones Unidas.

—La pretensión norteamericana, evidentemente contraria, en cuanto favorable al actual statu quo.

—Las posturas intermedias como la de la Unión Europea, que —al decir del propio Parlamento Europeo— propugna una representación democrática y geográficamente equilibrada de los órganos de gobierno de Internet, a la sazón insuficiente a su juicio, así como la no-interferencia de los gobiernos en su organización y gestión, respaldando la autorregulación como base de funcionamiento del organismo gestor de Internet,

ICANN, si bien de conformidad con los principios de la normativa internacional.

El conflicto aún dista de estar resuelto. Y, por ello, sigue también vivo el riesgo de que Estados poco respetuosos de los derechos humanos, la libertad de expresión muy singularmente, ganen capacidad de decisión en el gobierno de Internet, con fines de proyectar al conjunto de la Red regímenes internos de aquella índole.

Consideraciones tecnológicas

En el plano tecnológico, es por otra parte previsible que los patrones meramente técnicos marcados por toda esa serie de organismos recién citados, destacando de nuevo ICANN —aunque también ICCB o IAB, en lo que a los estándares y protocolos de comunicaciones respecta o el llamado World Wide Web Consortium (W3C)—, continúen durante cierto tiempo siendo la única referencia normativa, bien que en absoluto jurídica, por cuanto no se trata, como es conocido, de normas impuestas por un poder estatal o internacional.

Eso sí, su mero carácter técnico no debe en manera alguna hacer olvidar la enorme importancia de esta normativa: pautas técnicas como las de regulación de los nombres de dominio, o el mencionado protocolo TCP/IP, por ejemplo, son absolutamente capitales para el mismo desenvolvimiento de la Red: sin ellas, Internet simplemente no podría funcionar.

Retos de futuro para el derecho de internet

Conforme los primeros problemas de ajuste entre Internet y derecho se van asentando (inicial negación de toda virtualidad del Derecho en este campo y fuentes del mismo), comienza a atisbarse una nueva generación de retos legales para la Red.

1. El primero constituye un desafío directo a la Internet abierta o neutral. Se trata de la llamada calidad de servicio como posible título habilitante para gestionar las redes de comunicaciones electrónicas, en particular su ancho de banda. En otros términos, que operadoras de comunicaciones electrónicas puedan

estar facultadas para dar prioridad a unos tráficos sobre otros en Internet con la excusa de evitar interferencias (parece razonable) o de favorecer sus servicios sobre los de la competencia (ya no lo parece tanto). Por ello, y a mi entender, es justamente en la calidad de servicio donde el principio de neutralidad de la Red se juega hoy por hoy su destino.

2. En segundo lugar, y a pesar de las limitaciones de la regulación internacional del ciberespacio, ya expuestas, empieza a abrirse paso un nuevo subsector del derecho de la Red, que algunos vienen denominando Derecho internacional de Internet. Así se desprende por ejemplo de la creciente relevancia en el actual mundo multipolar de temas como la citada gobernanza del ciberespacio.

O de la cada vez más necesaria regulación planetaria de la ciberguerra. Ese gran acuerdo internacional sobre ciberdefensa debiera afrontar asuntos como: la proporcionalidad de los medios que se empleen, en función de la intensidad del ataque sufrido; la protección de los objetivos civiles, uno de los elementos clave de la regulación de la guerra «tradicional», y que en este contexto cobra por razones evidentes una importancia capital; la legitimidad o no de acciones defensivas «preventivas», cuestión polémica por excelencia en este campo; o finalmente, cuantas medidas contribuyesen a evitar la «militarización de la Red» [38], un riesgo de consecuencias obviamente nefastas para la libertad.

3. No en vano, y con ello pasamos al tercer punto, Internet constituye el principal escenario de desarrollo y amenaza para los derechos y libertades en nuestro tiempo. Tres son los derechos que, como la experiencia ha demostrado y más atrás se afirmaba, más afectados se han visto por la expansión de Internet: libertad de expresión, privacidad en todas sus manifestaciones (intimidad, imagen, protección de datos, etc.) y propiedad intelectual e industrial. Lo curioso en este sentido es que Internet ha venido propiciando, no solo esa afectación de estos tres derechos por se-

38. Véase Crawford, S., «The Militarization of the Internet», *Circle ID,* 20 de octubre de 2010, http://www.circleid. com/posts/20101020_the_militarization_of_the_internet.

parado, sino el choque entre ellos, al que de por sí son proclives. A buen seguro que los años venideros serán testigos de un análisis cada vez más profundo de esas interrelaciones y conflictos.

4. El cuarto frente de interés lo constituye la responsabilidad de los intermediarios, entendiendo por tales los proveedores de servicios de acceso y los de búsqueda y contenidos. La omnipresencia de estas entidades en las operaciones que cualquier usuario realiza en Internet hace que tarde o temprano puedan verse involucradas en conflictos generados por aquél.

A raíz de ello, éste de la responsabilidad de los intermediarios supone sin duda uno de los temas horizontales por excelencia del Derecho de la Red. Además de por lo dicho, porque es uno de los temas absolutamente originales de esta disciplina: sin Internet, no existiría como tal. Segundo, porque, aunque existen normas que lo regulan (en Europa, la Directiva 2000/31/CE sobre comercio electrónico, desarrollada en España por la Ley 34/2002 sobre ese mismo asunto), y ya abundante jurisprudencia que lo viene perfilando, es problema siempre matizable en función de las singularidades tecnológicas del ciberespacio, a la vez en permanente y veloz evolución, así como de múltiples circunstancias singulares, entre ellas la propia actitud del intermediario en cuestión.

Tercero, porque este régimen de responsabilidad condicionará a su vez de modo esencial el ejercicio de derechos y libertades en la Red: una responsabilidad potencialmente draconiana para los intermediarios haría que éstos restringieran con excesiva prevención los contenidos que un usuario pudiera llegar a verter en Internet, con el consiguiente empobrecimiento general.

5. Los problemas de jurisdicción suponen el quinto frente de retos de futuro. De hecho, esta cuestión es probablemente la de más compleja solución de cuantas se ha venido afrontando en este campo. Constatadas las limitaciones de la regulación internacional, no queda otro remedio que acudir a los Estados o a las regiones que como la Unión Europea aglutinan a diversos de ellos, para encontrar normas que aporten soluciones a un problema particular. Puede no obstante suceder que los autores de un ciberataque, pongamos por caso, no estén presentes en el Estado cuyas leyes se hayan de aplicar al mismo, ni posean en él bienes, ni exista tratado alguno de extradición que vincule al

país que juzga con el país en que el infractor se encuentre [39]. El Derecho de Internet no ha sido aún capaz de aportar soluciones que permitan sortear satisfactoriamente uno y otro escollo.

6. El sexto y último filón de desafíos legales del entorno digital viene marcado por las tecnologías Big Data. Por supuesto, éstas traen consigo enormes oportunidades de avance tecnológico y social, aunque también grandes riesgos, en tres líneas principales:

—Primero, y de la mano del cloud computing, la recreación de nuevas barreras que subviertan la apertura de Internet. Tim Berners-Lee [40] es probablemente el principal denunciante de este problema, que identifica con la construcción de verdaderos «silos» inconexos de información por parte de las grandes empresas de Internet. Derechos como la portabilidad de los datos entre distintas plataformas, que por ejemplo prevé la próxima reglamentación de datos de la Unión Europea, se revelan aquí fundamentales.

—Segundo, riesgos de ciberseguridad, crecientes al serlo también el volumen de datos en circulación y la calidad de su tratamiento. La regulación del ciberdelito deberá pues acentuar su concentración en este contexto.

—Y tercero, riesgos en aumento para la privacidad de las personas, derivados de la imparable inmersión de todos y cada uno de nosotros en el envolvente entorno de una Internet cada vez más «total» [41].

39. Véase Post, D.G., *In Search of Jefferson´s Moose…, op. cit.*

40. Véase Berners-Lee, T., «Long Live the Web: A Call for Continued Open Standards and Neutrality», *Scientific American Magazine*, diciembre de 2010, http://www.scienti_camerican.com/article.cfm?id=long-live- the-web&print=true.

41. Véase García Mexía, P., *Historias de Internet. Casos y cosas de la Red de redes, op. cit.*, págs. 160-164.

INTERNET Y EL USO DE LA FUERZA

Soledad Torrecuadrada García-Lozano*

Introducción

El título de este trabajo está formado por dos elementos que se encuentran en un equilibrio inestable. Por una parte, el uso de la fuerza de cuya regulación positiva en el artículo 2.4 de la Carta se viene anunciando la defunción desde hace más de cuarenta años, cuando publicó Thomas Franck su artículo titulado «Who Killed Article 2(4)? or: Changing Norms Governing the Use of Force by States» [1]. El argumento desarrollado a estos efectos encuentra fundamento en la falta de congruencia entre el contenido jurídico de aquel precepto y el interés de los Estados, constatando que en caso de conflicto entre ellos vence el indicado en último lugar. Más recientemente, Michael J. Glennon [2] reiteraba la defunción del artículo 2.4, en este caso por desuetudo consecuencia de las violaciones de las que ha sido objeto. Este resultado, sin embargo, no resulta plausible al ignorar los numerosos supuestos de cumplimiento. Ambas argumentaciones conducen a los internacionalistas a lugares comunes, en los que se cuestiona la falta de eficacia del Derecho Internacional atendiendo a la vulneración de sus normas, aún cuando las estadísticas contradicen la afirmación sobre la que se edifican.

* Soledad Torrecuadrada García-Lozano es Profesora Titular de Derecho Internacional Público y Relaciones Internacionales en la Universidad Autónoma de Madrid.

1. Véase Franck, Thomas M., «Who Killed Article 2(4)? or: Changing Norms Governing the Use of Force by States», *American Journal of International Law*, vol. 64, núm. 5, (1970), págs. 809 y ss.

2. Véase Glennon, Michael J., «How International Rules Die», *Georgetown Law Journal,* vol. 93, (2005), págs. 939 y ss.

En el otro extremo de la balanza nos encontramos con un elemento claramente emergente: las nuevas tecnologías y su desarrollo, no solo como una herramienta imprescindible en la actualidad para casi cualquier actividad, sino también como instrumento bélico empleado con el propósito de atacar los servicios básicos del Estado que dependen de aquellas. Es lo que se ha dado en denominar la ciberguerra. Con carácter general, la evolución de la red y de sus potencialidades ha conseguido transformar internet que, en muy poco tiempo ha pasado de ser un elemento con una evidente utilidad instrumental a convertirnos casi en sus esclavos.

La revolución tecnológica no solo ha alterado los patrones de comportamiento individual sino que sumada a la mundialización ha producido, como afirma Anna Badía, un cambio en la sociedad internacional [3], en una suerte de democratización tecnológica. Si las normas que rigen las relaciones entre los sujetos que conforman las sociedades han de poseer capacidad de adaptación a las nuevas características o problemas societarios, en la actualidad, el dinamismo predicable de la realidad en este punto dificulta considerablemente la adaptabilidad normativa, tanto a esos nuevos perfiles en constante cambio como al diseño de la posible reacción a las amenazas de las que es destinataria.

En relación a esta última cuestión resulta ilustrativo el comienzo de un artículo firmado por Sharon R. Stevens. En esas primeras líneas la autora nos pide realizar un ejercicio de imaginación: estamos en el año 2015 y un grupo de personas utiliza intenet para atacar el sistema de control del tráfico aéreo en el aeropuerto de Heathrow, en un intento de visualizar las consecuencias directas e indirectas que de esta situación podrían derivar [4]. Todo ello con el

3. Véase Badía Martí, A. M., «Las nuevas tecnologías ante el ordenamiento jurídico internacional», en Hinojo Rojas, Manuel (coord.) *Liber amicorum Profesor José Manuel Peláez Marón. Derecho Internacional y Derecho de la Unión Europea*, Servicio de Publicaciones de la Universidad de Córdoba, Córdoba (2012), pág. 93 y ss.

4. Véase Stevens, Sharon R., «Internet War Crimes Tribunals and Security in an Interconnected World», *Transnational Law & Contemporary Problems*, vol. 18 (2009), pág. 658.

propósito de concienciarnos de las vulnerabilidades derivadas de la dependencia informática que caracteriza a las infraestructuras básicas del Estado. Esta situación plantea dos caras de una misma moneda: por una parte, muestra de las capacidades estatales; por otra, emerge como un flanco de fragilidad si no se acompaña de los imprescindibles esfuerzos de inversión en posibles cortafuegos o sistemas de protección frente a eventuales ataques [5].

Resulta evidente que si los servicios públicos básicos (además de los militares) dependen de la informática pueden destruirse o inutilizarse, aunque sea temporalmente, mediante virus, con lo que parece que la práctica ha hecho realidad la ficción contemplada en algunas películas con descreimiento. Por lo demás, el dinamismo característico de las potencialidades de internet en constante evolución, provoca que los cortafuegos o mecanismos de protección no garanticen un blindaje absoluto y atemporal frente a sus posibles amenazas, puesto que siempre podemos encontrar *hackers* empeñados en estudiar las vulnerabilidades de los sistemas para detectar nuevos flancos expuestos con el propósito de atacarlos. Un intento de reducir este riesgo condujo al Ministro de Telecomunicaciones iraní a anunciar, en agosto de 2012, que los principales organismos de su gobierno sustituirían la conexión a través de Internet por una intranet [6].

En todo caso, la realidad confirma las palabras de Matthew Waxman quien recientemente afirmaba que la impermeabilidad a este tipo de amenazas no guarda una relación proporcional con las capacidades estatales (políticas, económicas o militares), pues normalmente a menor dependencia menor exposición [7].

5. Sobre los tipos de ciberataques y su potencial impacto destructor, de forma sintética y clara, véase Sklerov, Matthew J., «Solving the Dilema of State Responses to Cyberattacks: A Justification For the Use Of Active Defenses Against States Who Neglect Their Duty to Prevent», *Military Law Review,* vol. 201 (2009), págs. 1 y ss, especialmente págs. 13 a 21.

6. Ver información al respecto en: http://actualidad.rt.com/actualidad/view/50894-Ir%C3%A1n-se-desconectar%C3%A1-de-Red-para-protegerse-de-ataques

7. Véase Waxman, Matthew C., «Cyber-Attacks and the Use of force: Back to the future of article 2(4)», *The Yale Journal of International Law,* vol. 36 (2011), pág. 451.

Aunque cabe también que esa menor dependencia sin inversión en protección pueda extremar la fragilidad de aquellos servicios controlados mediante sistemas informáticos. Evidentemente en este ámbito material cuanto mayor sea la utilización de la red mayor será la vulnerabilidad, por cuanto los flancos expuestos a potencial riesgo se multiplican.

Por otra parte, las infraestructuras estatales se caracterizan por su interconexión, lo que «create security risks because the internet utilizes an open architecture based on the free flow of information» [8]. En consecuencia, la que es la principal ventaja de la red (su apertura) se convierte en la mayor debilidad en lo que a su protección se refiere (el acceso de virus que colapsen, reprogramen, inutilicen o destruyan el sistema), multiplicando la capacidad de afectación debido a su circulación por esa red que comunica los servicios conectados [9].

Las páginas de la prensa nos ilustran acerca de la proliferación *in crescendo* de los ataques informáticos así, en 2008 ya se advirtió de la posibilidad de un denominado 11-S digital [10]. Más recientemente, según los datos hechos públicos por la Comisión Europea durante 2011 aquellos ataques crecieron un 36% en la UE [11], dato que ilustra la tendencia alcista de los últimos años. En Estados Unidos el número de ciberataques a infraestructuras estatales se multiplicó por diecisiete entre 2009 y 2011, aunque desconocemos

8. Véase Stevens, Sharon R., «Internet War Crimes Tribunals and …», *loc. cit.*, *supra* nota núm. 4, pág. 661.

9. En este sentido, Liff, Adam P., «Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War», *The Journal of Strategic Studies*, vol. 35, núm. 3 (2012), págs. 401 y ss. En pág. 426, afirma que posiblemente los ataques cibernéticos no son, por el momento, el nuevo 'absolute weapon', pero innegablemente implica una multiplicación de los ataques.

10. Véase al respecto: *Annual Incident Reports 2011. Analysis of the Article 13.ª reports of 2011*. Octubre 2012, en http://www.enisa.europa.eu/

11. Es una información difundida por la agencia de noticias EFE el 23 de julio de 2012, en http://economia.elpais.com/economia/2012/07/23/agencias/1343044404_606121.html. En concreto, la Comisión y el Servicio Exterior de la UE fueron víctima de serios ciberataques, tal y como se publicó, entre otros, en *El Mundo*, en http://www.elmundo.es/elmundo/2011/03/24/navegante/1300961999.html.

qué porcentaje concreto afectó a elementos críticos de la infraestructura del país [12]. En enero de 2010 nos enteramos que en 2009 instituciones y organismos clave españoles fueron víctimas de más de cuarenta incidentes graves [13]. Incluso en 2009 se produjeron dos ciberataques contra el Centro Nacional de Inteligencia (CNI) y otros dos contra el Centro Criptográfico Nacional.

De esas vulnerabilidades no están a salvo los particulares (operación Mariposa [14]), los Ministerios estatales [15] o las industrias militares japonesas [16], por citar solo algunos ejemplos [17] que nos permiten visualizar la generalidad material de los ataques y vulnerabilidades. Tampoco respetan límites subjetivos pues, como indicaba la Comisión Europea, se trata de amenazas colectivas debido precisamente a la interconexión general de los sistemas, y de forma más concreta, de los utilizados por los servicios estatales [18],

12. Véase en *ABC* de 29 de julio de 2012, en http://www.abc.es.

13. Véase Elola, Joseba, «España, blanco de más de cuarenta ciberataques», en *El País* de 24 de enero de 2010, en http://elpais.com/diario/2010/01/24/domingo/1264308753_850215.html.

14. Aplicaciones informáticas con las que conseguían acceder y utilizar remotamente los ordenadores que infectaron a más de 12 millones de terminales, véase información al respecto en: http://www.elmundo.es/elmundo/2010/03/02/navegante/1267545550.html.

15. Quizá uno de los más conocidos es el ataque contra el Ministerio de economía francés en marzo de 2011, véase información al respecto en http://internacional.elpais.com/internacional/2011/03/07/actualidad/1299452406_850215.html.

16. Véase http://tecnologia.elpais.com/tecnologia/2011/09/21/actualidad/1316595663_850215.html.

17. En algunas ocasiones las amenazas, debido a la subjetividad que las caracteriza, quedan en una difuminada frontera entre el rumor y la amenaza propiamente dicha. Encontramos un ejemplo en el temor de Gibraltar, publicado en los medios de comunicación, de ser víctima de un ataque cibernético atribuible a las autoridades españolas (Véase en http://www.publicserviceeurope.com/article/2226/heightened-tensions-on-the-rock-of-gibraltar). Finalmente, en los últimos días del mes de julio de 2012 la amenaza se materializó en un apagón de cuatro horas como consecuencia de un supuesto fallo en los generadores eléctricos que no afectó a los servidores de internet. Por tanto, la amenaza publicada, en realidad no fue sino un rumor.

18. La Comisión Europea en su Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de información «logros y próxi-

lo que provoca que potencialmente puedan extender su radio de acción sin límites físicos. Por ello, emerge con fuerza la necesidad de la coordinación y cooperación para prevenir y neutralizar los efectos de un posible ataque por este medio [19].

En este contexto surgen cuestiones como las siguientes ¿esos ataques cibernéticos pueden considerarse una materialización del uso de la fuerza? De ser así ¿sería un uso de la fuerza lícito? Y, en consecuencia ¿susceptible de desencadenar una reacción con fundamento en la legítima defensa? ¿hay que regularlos? ¿de qué modo?, a las que intentaremos dar respuesta en las páginas siguientes.

¿Pueden considerarse los ciberataques como una materialización del uso de la fuerza?

Como avanzó Duncan B. Hollis, la «use of force prohibition encounters real difficulty, however, when translated into the Information Operation context» [20]. En particular, para poder considerar los ataques cibernéticos como una materialización del uso de la fuerza hemos de superar dos dificultades: una, la falta de una definición positiva de lo que es el uso de la fuerza con todas sus posibles aristas; dos, la identificación de los posibles comportamientos que, realizados a través de internet, pueden ser objeto de tal calificación [21].

---

mas etapas: hacia la ciberseguridad global», Bruselas 31 de marzo de 2011, COM (2011) 163 final, lo expresaba del siguiente modo, en relación a la situación en Europa: «Están surgiendo amenazas nuevas y más avanzadas tecnológicamente, con una dimensión geopolítica que, de forma cada vez más clara, es de carácter mundial»

19. Coordinación cuya utilidad ya se identificaba en el Libro Verde de la Comisión sobre un Programa Europeo para la protección de infraestructuras críticas, Bruselas 17 de noviembre de 2005, COM (2005) 576 final.

20. Véase Hollis, Duncan B., «Why States Need an International Law for Information Operations», *Lewis & Clark Law Review*, vol. 11 (2007), pág. 1040.

21. Para visualizar claramente los tipos de ataques informáticos y sus efectos, véase Liff, Adam P., «Cyberwar: a New 'Absolute Weapon'? …», *loc. cit.*, *supra* nota núm. 9, págs. 406 y ss., que incorpora una tabla clara y muy fácil de entender para profanos en cuestiones técnicas.

En relación a la primera de las dificultades apuntadas hasta fechas muy recientes resultaba evidente que el alcance del concepto «uso de la fuerza» se circunscribía en exclusiva a la fuerza armada [22]. Es cierto que, cuando nos referimos al principio que consagra su prohibición acudimos a la Carta de Naciones Unidas y, de modo más concreto, a su artículo 2.4 cuya redacción cuenta ya con casi setenta años y no concreta a qué tipo de fuerza se refiere. Además, sabemos que, en aquel momento, se propuso sin éxito alguno que la prohibición alcanzara a cualquier tipo de fuerza no exclusivamente armada, Brasil defendía la incorporación de la presión económica, Ecuador de la fuerza moral o física e Irán la fuerza política [23]. Desde entonces, la interpretación de este precepto, se reduce a la fuerza militar, el resto de presiones (políticas, económicas u otras…) serían, en su caso, constitutivas de un acto de intervención [24].

Con el propósito de interpretar el alcance de la prohibición podemos acudir a la jurisprudencia de la Corte Internacional de Justicia [25] y a algunas resoluciones de la Asamblea General de Na-

22. Así lo establecen los comentaristas de la Carta, véase en este sentido Randelzhofer, A., «Article 2(4)», en Simma, B., (coord.), *The Charter of the United Nations. A Commentary*, Oxford University Press, 2.ª ed. (2002), pág. 112 y ss. o Schrijver, N., «Article 2. Paragraphe 4», en Cot, J.-P., Pellet, A. & Forteau, M. (eds.), *La Charte des Nations Unies. Commentaire article par article,* ed. Economica/ Bruylant, París/Bruselas, (2005), págs. 437 y ss.

23. *Id.* nota anterior.

24. Encontramos una materialización de esta interpretación en el artículo 41 de la Carta que excluye de la consideración de medidas que implican el uso de la fuerza, con carácter ejemplificativo la interrupción total o parcial de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas.

25. Con carácter general pensaremos en una Sentencia y una Opinión consultiva que resultan relevantes a estos efectos: la de 27 de junio de 1986, en el asunto de las actividades militares y paramilitares en y contra Nicaragua (Nicaragua c. Estados Unidos), dictada hace más de veintiséis años (http://www.icj-cij.org/docket/files/70/6502.pdf), en la que se interpretó y aplicó la norma consuetudinaria que prohíbe la amenaza y el uso de la fuerza y no la norma convencional incorporada en el artículo 2.4 de la Carta; y la Opinión Consultiva, formulada diez años después, de 8 de julio de 1996, sobre la licitud de la amenaza o el empleo de armas nucleares (vid. en http://www.icj-cij.org/docket/files/95/7494.pdf)

ciones Unidas adoptadas en la década de los años setenta (como la 3314 [XXIX] o la 2625 [XXV]), en las que se identifican actos constitutivos de vulnerar la prohibición atendiendo a los que se producían en aquella época, cuando los ciberataques pertenecían al mundo de la fantasía.

Podemos acudir a la definición de «agresión», para ver si los ciberataques podrían considerarse de este modo pero, si tomamos como parámetro definidor la Resolución 3314 (XXIX) de la Asamblea General [26], la respuesta inicial será negativa por dos razones: la primera subjetiva y la segunda material. Subjetiva, pues identifica al autor de los comportamientos tipificados como «agresión» con las fuerzas armadas o, en su defecto, al propio Estado, lo que nos ubica en ataques armados exclusivamente atribuibles a este sujeto (vid. infra); material, puesto que las actuaciones incorporadas tienen como propósito la ocupación o anexión de un territorio, su bombardeo, el bloqueo de puertos o costas, entre otros [27], efectos

26. La Resolución 3314 (XXIX), de 14 e diciembre de 1974 puede verse en http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/743/93/IMG/NR074393.pdf?OpenElement

27. El artículo 3 establece:

La invasión o el ataque por las fuerzas armadas de un Estado del territorio de otro Estado, ó toda ocupación militar, aun temporal, que resulte de dicha invasión o ataque, o toda anexión, mediante el uso de la fuerza, del territorio de otro Estado o de parte de él; b) El bombardeo, por las fuerzas armadas de un Estado, del territorio de otro Estado, o el empleo de cualesquiera armas por un Estado contra el territorio de otro Estado; c) El Bloqueo de los puertos o de las costas de un Estado por las fuerzas armadas de otro Estado; d) El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres, navales o aéreas de otro Estado, o contra su flota mercante o aérea; g) La utilización de fuerzas armadas de un Estado, que se encuentran en el territorio de otro Estado con el acuerdo del Estado receptor, en violación de las condiciones establecidas en el acuerdo o toda prolongación de su presencia en dicho territorio después de terminado el acuerdo; f) La acción de un Estado que permite que su territorio, que ha puesto a disposición de otro Estado, sea utilizado por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado; g) El envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación en dichos actos.

Se trata de un listado que el Consejo de Seguridad puede ampliar.

que, por el momento, no persiguen los ataques informáticos a los que nos referimos [28].

La práctica del Consejo de Seguridad no nos ayuda tampoco en este punto, puesto que su estudio no permite identificar como uso de la fuerza la utilización de internet. También podemos infructuosamente estudiar la práctica de este órgano político de Seguridad, con el propósito de identificar las ocasiones en las que emplea el término «uso de la fuerza», extrayendo criterios que nos permitan avanzar en la definición del concepto atendiendo al contenido. Sin embargo, cuando ha autorizado el uso de la fuerza armada, como en el caso de la resolución 678 (1990), de 29 de noviembre, se ha referido a todos los medios necesarios para conseguir el fin pretendido que, en aquella ocasión no era sino el punto final a la anexión de Kuwait por parte de Iraq, omitiendo mencionar el uso de la fuerza.

Por su parte, el Secretario General se refiere a «uso de la fuerza militar» en su Informe «Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos» [29]. En este documento, Kofi Annan plantea si el genocidio, la depuración étnica y otros crímenes similares de lesa humanidad podrían considerarse amenazas para la paz y la seguridad internacionales, guardando silencio sobre la posible utilización de internet con este propósito.

En relación a la segunda dificultad aludida al inicio de este epígrafe (la identificación de los posibles comportamientos que, realizados a través de internet, pueden ser objeto de tal calificación), es sobradamente conocido el potencial de la red como medio de comunicación. En este sentido, solo nos hace falta contemplar los graves disturbios que se han producido como

28. Los problemas que plantea la aplicación del concepto «agresión» a los ataques cibernéticos provoca que Ophardt, Jonathan A., «Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield», *Duke Law & Tecnology Review,* núm. 3 (2010), págs. 1 y ss., defienda la necesidad de definir el crimen de agresión para adaptarlo a las nuevas necesidades, aprovechando también para superar las dificultades derivadas de la Resolución 3314 de la Asamblea General.

29. El informe completo puede verse en http://www.un.org/spanish/largerfreedom/summary.html. La referencia aludida en el texto figura en el parágrafo 122, pág. 36.

consecuencia del video difundido en *youtube* en el que se ridiculiza a Mahoma titulado 'La inocencia de los musulmanes', o la utilización de las redes sociales como instrumento difusor de manifestaciones o disturbios, incluso en un artículo reciente se publicaba la relevancia de estos medios en la organización del denominado «Ejercito Libre de Siria» [30].

Este potencial no es novedoso, pues como ha escrito el Profesor Antonio Segura, en la campaña de la OTAN contra Yugoslavia en 1999 la Organización atacó como objetivos militares algunas instalaciones de Internet en Belgrado, con el propósito de neutralizar las infraestructuras de comunicación [31]. Es la identificación de la importancia del elemento cibernético en el transcurso de un conflicto armado [32], aunque todavía no su utilización como arma sino como objetivo militar.

En marzo de 2010 el director del FBI, Robert Mueller advertía que «un ciberataque podría tener el mismo impacto que una «bomba bien colocada»» [33]. Si esto es así, podríamos encontrarnos ante ataques prohibidos por el artículo 2.4 de la Carta. Es cierto que hay comportamientos que no dejan lugar a dudas, pues resulta meridianamente evidente que algunas actividades, desarrolladas total o parcialmente a través de internet, se ven alcanzadas por el concepto clásico de uso de la fuerza [34]. Es el caso de los drones,

30. Véase «La lucha de la ciber-yihad», publicado en el diario *La Razón*, el 2 de agosto de 2012, en http://www.larazon.es/noticia/5966-la-lucha-de-la-ciber-yihad.

31. Segura-Serrano, A., «Internet Regulation and the Role of International Law», *Max Planck UNYB,* 10 (2006), pág. 221.

32. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue y Julia Spiegel firman un extenso e interesante estudio titulado «The Law of Cyber-Attack», publicado en *California Law Review*, vol. 100 (2012), págs. 816 y ss, en el que incorporan una definición de ciberataque, justificando cada uno de los elementos que la componen (entre las páginas 826 y 832), es la siguiente «A cyber-attack consists of any action taken to undermine the function of a computer network for a political or national security purpose».

33. Véase Reuters «El FBI advierte de la creciente amenaza de ciberataques», en *ABC*, 5 de marzo de 2010.

34. Nos alejamos aquí de quienes niegan la posible consideración de los ciberataques como uso de la fuerza debido a la ausencia de cualificación del medio electrónico como uso de la fuerza debido a la falta del instrumento militar (véase Kanuck, Sean P., «Information Warfare: New Challenges for Public

aviones no tripulados (UAV por sus siglas en inglés [35]) cuyo enlace vía satélite puede ser hackeado, por lo que quien accediera a este sistema no solo tendría la posibilidad de inutilizarlos sino también de reprogramarlos para que utilicen la fuerza armada y, en esa medida no habría dudas sobre la calificación que el hecho merece.

Existen otros supuestos igualmente poco dudosos, como la organización y adiestramiento de bandas armadas para «hacer incursiones» en otro Estado, que la resolución 2625 (XXV) de la Asamblea General considera una manifestación de uso de la fuerza armada prohibida. Estos comportamientos, en la actualidad, se desarrollan o pueden desarrollarse a través de Internet, incluso si buscamos en los tutoriales de *youtube*, encontraremos el adiestramiento necesario para ello [36].

En este punto, cabe plantear si, al margen de estos actos, no identificaríamos otros ataques cibernéticos que puedan considerarse arma atendiendo a sus consecuencias [37]. Si contemplamos la

---

International Law», *Harvard International Law Journal*, 37 (1996), págs. 272 y ss. especialmente págs. 288-289. En el mismo sentido podemos leer a DiCenso, Maj David J., «Information Operations: An Act of War?», en *Air & Space Power Journal*, documento de 31 de julio de 2000, puede consultarse en la siguiente dirección: http://www.airpower.maxwell.af.mil/airchronicles/cc/dicenso1.html), al parecernos más convincente la posición entre otros de Dinstein, Yoram, «Computer Network Attacks and Self-Defense», en Schmitt, Michael N. y O'Donnell, Brian T., (eds.) *Computer Network Attack and International Law*, Naval War College, Newport (2002), págs. 99 y ss.

35. Véase http://www.wired.com/dangerroom/2009/06/strategist-killer-drones-level-extremists-advantage/.

36. El texto de la resolución en este punto es el siguiente:

Todo Estado tiene el deber de abstenerse de organizar o fomentar la organización de fuerzas irregulares o de bandas armadas, incluidos los mercenarios, para hacer incursiones en el territorio de otro Estado.

Todo Estado tiene el deber de abstenerse de organizar, instigar, ayudar o participar en actos de guerra civil o en actos de terrorismo en otro Estado, o de consentir actividades organizadas dentro de su territorio encaminadas a la comisión de dichos actos, cuando los actos a que se hace referencia en el presente párrafo impliquen el recurrir a la amenaza o al uso de la fuerza.

37. Lo que supone identificar el elemento instrumental al que se refiere Clausewitz, con el que derrotar al enemigo o al menos causarle un evidente daño.

resolución 3314 (XXIX) observamos que los efectos derivados de los comportamientos constitutivos de agresión en aplicación de su artículo 3 [38] puedan igualmente alcanzarse utilizando medios cibernéticos, lo que nos inclina a responder afirmativamente a su consideración como actos de agresión, aunque no se realicen por fuerzas armadas de un Estado, como afirma expresamente la Resolución recién indicada. Una interpretación diferente supondría escudarse en una formalidad para evitar las consecuencias de un hecho exclusivamente atendiendo no a criterios de atribución al Estado, sino al tipo de relación existente entre el autor y este último que parece difícilmente defendible en la medida en que sea posible establecer la relación entre la autoría material del hecho en cuestión y el Estado al que se atribuye.

Junto con estos comportamientos de los que derivan efectos idénticos al uso de la fuerza armada entendida en sentido clásico o que se verían alcanzados materialmente por el concepto de agresión, existen otros dudosos. De ahí la necesidad de concretar qué tipo de actos pueden ubicarse en nuestro ámbito de estudio. En este sentido, no vamos a considerar todos los virus informáticos, sino tan solo aquellos que pueden causar un efecto similar al de un ataque armado, susceptibles de producir la inutilización prolongada cuando no definitiva de un servicio militar o básico (que no suponga la caída breve o puntual del sistema), y que esos efectos resulten contrastables objetivamente. Lo anterior expresa la necesidad de un mínimo de gravedad en las consecuencias del ataque y nos conduce a apartar del foco de atención aquellos que no dudaríamos excluir de calificar como «uso de la fuerza» cuando se instrumentaliza por una vía diferente de internet. Es el caso de los actos de espionaje, robo de datos (aunque sean bancarios [39]), de mapas… cuya utilización puede provocar daños

38. Cuya redacción se transcribió *supra* en nota núm. 27.

39. Véase el comunicado de prensa de la Comisión Europea de 9 de julio de 2012, sobre la preocupación de los ciudadanos de la UE por la seguridad de la información personal y los pagos en línea. Soc. IP/12/751. El informe completo del Eurobarómetro junto con los datos desglosados por Estados puede verse en http://ec.europa.eu/public_opinion/archives/eb_special_399_380_en.html#390.

potencialmente graves, pero que carecen del efecto destructor característico de un ataque armado.

En este punto, recordemos la afirmación de Antonio Segura, según la cual ni toda utilización «maliciosa» de internet puede considerarse siempre un uso de la fuerza ni hay que descartarlo de forma automática [40]. En este sentido es preciso ponderar el caso concreto y la semejanza del daño producido con el que derivaría de un uso de la fuerza armada, tarea de equiparación que no siempre resulta fácil. Las respuestas generales normalmente resultan poco adecuadas para resolver problemas concretos y, en mayor medida, en el ámbito en el que nos encontramos pues intentamos aplicar categorías y consecuencias ideadas para una realidad muy diferente de la actualmente planteada.

Así, cuando un comportamiento de este tipo tiene efectos asimilables a del uso de la fuerza debemos considerarlo tal [41] aunque, a diferencia de los modelos clásicos de utilización de la fuerza militar cuyos efectos son visibles y comprobables por todos, en los virus informáticos no siempre ocurre de este modo. En consecuencia, la identificación de los resultados contiene una importante dosis de subjetivismo y no siempre resulta fácilmente constatable ¿cómo conocer objetivamente los efectos de un ataque? En unas ocasiones puede ser fácil, como cuando se produce una catástrofe en un medio de transporte, pero en otras tenemos que fiarnos de las afirmaciones de los implicados, que pueden coincidir … o no, para cuya ilustración nos basta un ejemplo: el caso del virus *Stuxnet*. Si su consecuencia fue la inutilización real del programa nuclear iraní, como afirmaban sus responsables [42],

40. Véase Segura-Serrano, A., «Internet Regulation …» *loc. cit., supra* nota núm. 31, pág. 223.

41. La consideración de la ciberguerra como tal es rechazada por Rid, Thomas, «Cyberwar will not take place», *The Journal of Strategic Studies*, vol. 35, núm. 1, (2012), págs. 5 y ss., en la medida en que no se encuentra en ella el tercer elemento establecido por Clausewitz: la violencia. Aunque es un elemento fácilmente rebatible acudiendo a los cambios profundos sufridos por los escenarios bélicos desde los casi dos siglos transcurridos desde esta caracterización.

42. Véase en este sentido: http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

sus efectos resultarían equiparables a los que derivaron del ataque israelí de 7 de junio de 1981 en la central iraquí de Osiraq [43] y, en consecuencia, a un uso de la fuerza [44].

Sin embargo, la víctima del ataque (Irán) desmintió inicialmente que hubiera afectado a la planta nuclear de Bushehr, incluso el Ministro iraní de telecomunicaciones Reza Taghipour, afirmaba que «Dado que usamos cortafuegos en los sistemas controlados por el Estado, este venenoso 'software' ha sido menos efectivo. No ha habido ningún daño importante» [45]. Como nada en esta vida puede ser una cosa y la contraria a un tiempo, resulta evidente que entre la destrucción de la que se vanagloriaban los autores y la minimización de la víctima hay un elevado número de posibilidades. En todo caso, parece evidente que desde que se lanzó el ataque informático el programa nuclear iraní se ha ralentizado. Lo anterior evidencia la dificultad de contrastar objetivamente el alcance de los efectos derivados de los ataques, encontrándonos ante valoraciones interesadas al respecto, quizá maximizándolos quienes lanzaron el virus (Israel y Estados Unidos) para que conozcamos su superioridad en este ámbito, mientras la víctima tienda a lo contrario reduciendo con ello su exposición y vulnerabilidad en este punto.

Otra cuestión a plantear es si esos ciberataques que, por los efectos que despliegan consideramos uso de la fuerza, serán lícitos o por el contrario, se encuentran proscritos por el artículo 2.4 de la Carta. En este sentido, hemos de aplicar la lógica del pro-

43. Véase una descripción de lo ocurrido en: http://news.bbc.co.uk/2/hi/middle_east/5020778.stm. La opinión oficial iraquí al respecto puede leerse en: http://ia600607.us.archive.org/16/items/TheIsraeliAggressionAgainstThePeacefulNuclearInstallationsInIraq/Isranuke.pdf. Véase D'Amato, A. defendiendo la licitud de la acción israelí: http://anthonydamato.law.northwestern.edu/Adobefiles/A961-Isr.pdf.

44. Adam P. Liff, en «Cyberwar : A New 'Absolute Weapon'…» *loc. cit., supra* en nota núm. 9, afirma que el virus *Stuxnet* es un ejemplo de *hacktivism* pero no de guerra, conclusión que alcanza por la aplicación de la caracterización de esta última de acuerdo con los elementos formulados por Clausewitz.

45. El texto transcrito corresponde a una noticia publicada el 27 de septiembre de 2010 en el diario El Mundo, en: http://www.elmundo.es/elmundo/2010/09/27/navegante/1285571297.html

pio artículo, los propósitos marcados en él, es decir los ataques cibernéticos en las relaciones internacionales contra «la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas», serán usos prohibidos. La formulación de la proscripción posee un alcance del que no podemos excluir a los ataques cibernéticos. Sabido es que las únicas excepciones a la prohibición, además de las contenidas en la Carta (el sistema de seguridad colectiva y la legítima defensa) ha sido la relativa a la consideración del uso de la fuerza en ejercicio del derecho a la libre determinación frente a las pretensiones negadoras de la potencia administradora [46]. En otros supuestos, como el de terrorismo precisamos de autorización del Consejo de Seguridad, mientras la predicada legítima defensa preventiva no es una excepción generalmente aceptada a estos efectos.

El problema de la atribución de los ciberataques

Una dificultad añadida a la consideración de los ciberataques como un uso de la fuerza deriva de su atribución a un Estado, pues la Carta prohíbe su empleo en las relaciones internacionales lo que nos conduce casi exclusivamente a aquel, aunque sin descartar a las Organizaciones internacionales. En consecuencia, el comportamiento en cuestión deberá ser atribuible a un sujeto de Derecho Internacional, normalmente a un Estado, siendo éste un aspecto que, aunque teóricamente pueda resultar fácil, goza en la práctica de una subrayada complejidad. El Proyecto de artículos de la CDI sobre responsabilidad internacional de los Estados [47] nos indica en qué supuestos los comportamientos ilícitos resul-

46. Lo que ha ocurrido sobre la base que proporciona el principio de libre determinación de los pueblos y la aplicación de la legítima defensa frente al ocupante que no es otro que la potencia administradora, en una materialización de un uso de la fuerza acorde con los propósitos y principios de la Carta de las Naciones Unidas.

47. Véase el Proyecto de Artículos sobre Responsabilidad del Estado por hechos internacionalmente ilícitos, adoptado por la CDI en su 53.º período de sesiones (A/56/10) y anexado por la AGNU en su Resolución 56/83, de 12 de diciembre de 2001.

tan atribuibles a los Estados. Así, cuando lo realiza un órgano del Estado (artículo 4), una persona que ejerce atribuciones del poder público y cuente con esa capacidad (artículo 5), quien actúa bajo la dirección y control del Estado (artículo 8) o bien aquel comportamiento que el Estado reconoce como propio (artículo 11), entre otros. Parece claro que, el virus *Stuxnet* encaja dentro de los criterios de atribución al Estado en la medida en que lo produjeron agencias estatales [48], aunque en otros supuestos no resulta tan evidente.

Desde esta perspectiva, el ataque que afectó a Estonia en mayo de 2007 nos sirve para ejemplificar una situación más que controvertida. Según se ha publicado, se trató de una serie de virus que provocó que los Ministerios estonios, la Presidencia del Gobierno, bancos, policía y dos de los diarios de mayor tirada quedaran sin conexión [49]. Al parecer, algunos de los IP desde los que se lanzó el ataque informático eran ordenadores del Kremlin, aunque el Financial Times, ha indicado que el ataque provenía de más de

48. Véase noticia de la confirmación en http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

49. Véase en http://www.forodeseguridad.com/artic/miscel/6060.htm:

El ataque fue en represalia porque el gobierno de Tallin desplazó a fines de abril desde el centro de la capital a un cementerio el Soldado de Bronce, un monumento erigido a los militares soviéticos caídos en el combate al nazismo, que para los estonios simboliza a quien ocupó durante medio siglo su país.

Los «hackers» rusos utilizaron la técnica del «zombie» que consiste en penetrar por una «puerta trasera» a una gran cantidad de computadoras en el mundo y de esa manera las «dominan» para reenviar desde allí millones de mensajes al mismo tiempo. De esa manera hacen colapsar cualquier sistema que ataquen.

En la casa de gobierno de Tallin se reciben de 1.500 a 2.000 mensajes por día. Desde fines de abril reciben 1.500 por segundo. El 1.º de mayo, el gobierno estonio tuvo que pedir a la población que se desconectara de Internet. Para entonces, el sitio del partido oficialista ya tenía la foto del premier Andrus Ansip con un bigote como el de Hitler, los bancos suspendieron por días las transacciones electrónicas y los diarios cortaron el acceso a sus páginas en la Red desde el exterior.

un millón de terminales [50] situados en 178 Estados [51]. Ante estas circunstancias, la atribución del hecho se complica, pues hemos de decidir si consideramos autores a todos ellos y de ser así, si a todos aquellos en cuyo territorio se encontraban ubicados los aparatos desde los que se lanzó (los 178) o solo a una parte y, en su caso, a cuáles de ellos.

Las autoridades estonias desde que comenzaron a sufrir los efectos del virus señalaron la autoría rusa, debido a la ubicación de alguna IP de los terminales desde los que se lanzó [52]. A pesar de lo anterior, hemos de tener en cuenta que las actividades desarrolladas por los particulares (aunque sea en el interior de los edificios oficiales) exclusivamente resultan atribuibles al Estado cuando sus autores actúan en ejercicio de las funciones que les son propias o lo hacen por cuenta y bajo la dirección de aquel, lo que no consta que ocurriera en el supuesto que nos ocupa. En este sentido, hay que ser cauteloso con la atribución de los comportamientos, pues si bien es cierto que los avances tecnológicos pueden hacernos replantear algunas relaciones afianzadas, no podemos obviar que esos mismos adelantos son susceptibles de provocar una innecesaria confusión. Por ello, si es posible la utilización remota de los terminales informáticos, podemos cuestionar hasta qué punto es fiable la identificación de la IP para atribuir ataques informáticos si pueden activarse desde otros.

En todos los casos hemos de identificar la conexión necesaria que nos permita relacionar claramente el terminal desde el que se lanza el ataque informático con el Estado al que pretendemos atribuírselo. Es preciso aplicar los criterios previstos en el Proyecto de artículos de la CDI sin buscar atajos para proporcionar cobijo a apreciaciones desmesuradas e interesadas en la mayoría

50. Véase Hollis, D.B., «Why States Need an International Law for Information Operations», *Lewis & Clark Law Review,* 11 (2007), pág. 2025.

51. Véase Clover, Ch., «Kremlin-Backed Group behind Estonia Cyber Blitz», *Financial Times*, 11 de marzo de 2009.

52. Véase http://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html. En sentido contrario, véase http://www.ordenadores-y-portatiles.com/ataque-hacker.html la información facilitada por quien se ha reconocido autor del hecho.

de los casos, que pretendan imputar a un Estado de este tipo de actuaciones.

El ataque a las infraestructuras estonias nos sirve también para ilustrar otra arista de la cuestión, pues según el *Washington Post* el gobierno ruso podría haber animado a los «hackers patrióticos» no gubernamentales para que desarrollaran esos comportamientos [53]. De comprobarse esta actitud podría influir en los criterios de atribución, aunque ser animado por ese aliento no es actuar por cuenta y bajo la dirección del Estado, lo que no debe entenderse como una negación de la responsabilidad estatal. Habría que analizar la repercusión del ánimo prestado, pues si bien no puede considerarse una ayuda o asistencia en la comisión de un hecho internacionalmente ilícito (artículo 16 del Proyecto de artículos de la CDI), claramente vulnera la obligación de prevenir un hecho ilícito (artículo 14.3 del mismo texto) [54].

Por otra parte, en la medida en que cualquier *hacker* puede, solo o en compañía de otros, producir daños desde su casa o desde un cibercafé en infraestructuras básicas o militares, como afirma Matthew C. Waxman [55], beneficiándose de que la información digital facilita el anonimato, la vulnerabilidad estatal se multiplica, pues no solo estamos expuestos a las acciones desarrolladas por Estados no demasiado amigos, sino también a la de esos *hackers* mañosos y esforzados que prueban sus capacidades. En estos supuestos parece complicado identificar la responsabilidad por negligencia estatal. Este anonimato podría impedir razonablemente a los Estados identificar a quienes están desarrollando virus con capacidad suficiente para provocar un ciberataque del

53. Véase Applebaum, Anne, «For Estonia and NATO, a New Kind of War», *Washington Post*, 22 de mayo de 2007. En el mismo sentido, véase Sanger, D.E., Markoff, J. & Shanker, Thom, «U.S. Plans Attack and Defense in Web Warfare», *New York Times,* 28 de abril de 2009.

54. Precepto este ultimo que, en concreto, establece lo siguiente:

3. La violación de una obligación internacional en virtud de la cual el Estado debe prevenir un acontecimiento determinado tiene lugar cuando se produce el acontecimiento y se extiende durante todo el período en el cual ese acontecimiento continúa y se mantiene su falta de conformidad con esa obligación.

55. Véase Waxman, Mattew C., «Cyber-Attacks and the use of force: Back to the Future of article 2(4)», *The Yale Journal of International Law,* vol. 36 (2011), pág. 444.

que derivaran efectos similares a los producidos por el uso de la fuerza armada y actuar con la debida diligencia. En esta medida difícilmente podríamos considerar la responsabilidad por negligencia estatal aplicando la doctrina establecida en la Sentencia de la toma de la Embajada y los consulados de Estados Unidos en Teherán [56]. Evidentemente, esto con la salvedad de aquellos que en virtud de tratados se hayan comprometido a actuar en un sentido determinado y no lo hayan hecho. Es el supuesto de los Estados parte en el Convenio sobre ciberdelincuencia de 2001 en el que se establece la obligación de tipificar y sancionar en su derecho interno estos comportamientos [57]. La vulneración de esta obligación implica incumplimiento del tratado, pudiendo considerarse también negligencia en este sentido.

La legítima defensa frente a los ciberataques

La preocupación por la consideración de los ataques informáticos dentro del alcance del tipo «uso de la fuerza» tiene carácter instrumental, ya que excede al interés real de la calificación, pues nos conduce a la consecuencia del uso de la fuerza: la legítima defensa que, Estados Unidos, en el asunto de Nicaragua, entendía como corolario directo y automático del uso de la fuerza. Frente a esta posición, la Corte Internacional de Justicia perfiló la existencia de condiciones para la aplicación de la relación, o lo que es lo mismo, que no siempre que hay un uso de la fuerza es posible el ejercicio de la legítima defensa, quedando restringida exclusivamente a los usos más graves de la fuerza [58].

56. Véase Sentencia de 24 de mayo de 1980 en el asunto relativo al personal diplomático y consular de Estados Unidos en Teherán (Estados Unidos c. Irán), en http://www.icj-cij.org/docket/files/64/6290.pdf

57. Es el Convenio adoptado en Budapest el 23 de noviembre de 2001, cuyo contenido puede leerse en: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF

58. Véase en este sentido la Sentencia en el asunto de las actividades militares y paramilitares en y contra Nicaragua, cuya referencia completa se encuentra en nota *supra* núm. 22. Sobre la legítima defensa en la jurisprudencia de la Corte Internacional de Justicia puede verse Green, James A., *The International Court of Justice and Self-Defence in International Law*, Hart Publishing, Oxford, (2009).

Para poder apreciar la presencia de la legítima defensa hemos de solventar con carácter previo los problemas de atribución referidos en el epígrafe anterior [59], debido a la íntima relación establecida entre la prohibición del uso de la fuerza y su excepción, pues se aplica en el contexto de una relación interestatal, por tanto, precisamos que el atacante sea un Estado [60].

Esto nos conduce a las condiciones de ejercicio de la legítima defensa que, como se refirió *supra*, cabe frente a los usos de la fuerza más graves, cuyo cumplimiento ha de producirse siempre que se pretenda acudir a esta categoría jurídica consolidada en el orden internacional. Esos requisitos son los de necesidad, proporcionalidad e inmediatez [61]. En cuanto al primero de ellos,

59. Es cierto que la legítima defensa tiene también virtualidad consuetudinaria. Sin embargo, cuando la doctrina apela a ella, lo hace para caracterizarla con los tintes que poseía en el caso Caroline de 1837 que se considera tradicionalmente la formulación «to be linked to the highly ambiguous legal norm of anticipatory self-defence with the consequence that its potential applicability to modern State» (Delibasis, Dimitrios, «State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century», *Peace Conflict and Development: An Interdisciplinary Journal*, Issue 8, febrero (2006), puede consultarse en http://www.peacestudiesjournal.org.uk). Por otra parte, es difícil visualizar la petrificación de la norma consuetudinaria, a pesar de los avances introducidos desde entonces tanto en la sociedad internacional como en el Derecho internacional y no solo porque un siglo después de aquel momento el Derecho Internacional clásico se transformara en contemporáneo, con todo lo que ello supuso.

60. Ello a pesar de que hay autores que afirman que cabe la legitima defensa contra actores no estatales, como es el caso de Wettberg, Gregor, *The International Legality of Self-Defense Against Non-State Actors. State Practice from the United Nations Charter to the Present*, Peter Lang, (2007), lo hacen fundamentando su posición sobre la práctica internacional que más que confirmar la extensión, se basan en un estudio de la práctica que, según el autor (pág. 21) «indicates a disregard for the formal nature of the attacking entity and thus never accepted this legal gap».

61. Sobre la legítima defensa, requisitos y condiciones de ejercicio existe una variada bibliografía, entre la más reciente puede verse: Rodin, David, *War and Self-defense,* Oxford University Press, 2.ª ed. (2004); Hensel, Howard M., *The Legitimate Use of Military Force. The Just War Tradition and the Customary Law of Armed Conflict,* Ashgate, (2007), Eyffinger, Arthur y otros (eds.), *Self-Defence as a Fundamental Principle,* Hague Academic Press, La Haya (2009); Ruys, Tom, *'Armed Attack' and Article 51 of the UN Charter. Evolutions in Costumary Law and Practice,* Cambridge University Press, (2010); o, Regueiro Dubra, Raquel, *La Legítima Defensa en Derecho Internacional*, Instituto Universitario General Gutierrez Mellado, Madrid (2012).

la necesidad, supone la inexistencia de alternativas pacíficas al uso de la fuerza para reaccionar frente al ataque del que estamos siendo objeto. En este sentido, Yoram Dinstein afirma que por este concepto hay que comprobar que el ataque:

> is no accident, to verify the genuine identity or the State —or non-State entity— conducting the attack (so as not to jeopardize innocent parties), and to conclude that the use of force as a counter-measures is indispensable. Should there be an opportunity to settle the matter amicably through negotiations, these must be conducted in good faith [62].

La inmediatez presenta escasas aristas especiales cuando nos referimos a los ciberataques, con la salvedad de la consideración del elemento temporal cuya apreciación puede complicarse si lo comparamos con el resto de los supuestos en los que se evalúa para la aplicación de la legítima defensa, como afirma Yoram Dinstein «since in cyberspace activities can produce reverberations around the world» [63]. De todos modos, en éste como en otros tipos de ataques hemos de distinguir entre la defensa aplicada frente a un ataque inminente y la legítima defensa preventiva que, por definición, no supone una aplicación de esta categoría jurídica, ubicándonos ante las medidas de autotutela [64]. En línea con el requisito de inmediatez, hay autores que defienden la aplicación de defensas activas que «consist of electronic countermeasures that attack an aggresive computer system, immobilizing that system and thus halting the cyber attack» [65], que reaccionan de for-

62. Véase Dinstein, Yoram, «Computer Network Attacks…», *loc. cit.*, *supra* nota núm. 34, pág. 109.

63. *Id.* nota anterior, pág. 110.

64. En este sentido véase Gibson, Dawn M., «A virtual Pandora's Box: Anticipatory Self-Defense in Cyberspace», en http://www.uniowa.edu/~cyberlaw/cs103/dgcs103.html. Schmitt, Michael, «Preemptive Strategies in International Law», *Michigan Journal of International Law,* 24, (2003) págs. 513 y ss. Especialmente entre las páginas 528 y 536, también puede entenderse el texto de Kesan, Jay y Hayes, Carol M., «Self-Defense in Cyberspace: Law and Policy», *Illinois Public Law Research Paper No. 11-16*, en http://ssrn.com/abstracr=1979857.

65. Graham, David E., «Cyber Threats and the Law of War», *Journal of National Security Law & Policy,* vol. 4 (2010), pág. 92.

ma agresiva, dañando el origen del mal que pretende afectarles. Estas defensas resultan perfectamente adecuadas al requisito que ahora nos referimos, dado que se activan al detectar un ataque ya desencadenado.

A diferencia de la necesidad y la inmediatez, la proporcionalidad suscita importantes cuestiones [66] pues relaciona la intensidad del ataque con su defensa. Con carácter general nos encontramos ante el elemento más difícilmente ponderable (la determinación del *quantum* necesario para repeler un ataque), máxime cuando pretendemos establecer el equilibrio entre factores disímiles por naturaleza. En este contexto, si bien resulta innegable que frente a un ataque informático de las características de aquellos a los que nos venimos refiriendo visualizamos más claramente la defensa simétrica mediante ataques cibernéticos que con armamento militar, como indica A. Remiro, no debemos descartar automáticamente esta posibilidad en la medida en que se considere la fuerza (cibernética o armada) necesaria para reprimir ese ataque previo y, en todo caso, siempre que se haya establecido la autoría estatal [67].

La falta de simetría entre el ataque y su defensa se pone también de manifiesto en las palabras de Walter Gary Sharp Sr. quien defiende que todos los ataques cibernéticos que causan efectos destructivos en el territorio de otro Estado es un uso de la fuerza ilícito de conformidad con el artículo 2.4 de la Carta, pudiendo aplicarse la legítima defensa como respuesta [68]. Consideración que para resultar compartida precisa de una matización, pues parece oportuna exclusivamente si para alcanzar esta conclusión

66. Sobre los problemas que plantea la proporcionalidad véase Wedgwood, Ruth G., «Proportionality, Cyberwar and the Law of War», Schmitt, Michael N. y O'Donnell, Brian T., (eds.) *Computer Network Attack and International Law*, Naval War College, Newport, (2002), págs. págs. 219 y ss.; y más recientemente Graham, David E., «Cyber Threats and the Law of War», *loc. cit., supra* nota núm. 65, págs. 87 y ss.

67. Véase en este sentido Remiro Brotóns, A. y otros, *Derecho Internacional. Curso general,* Tirant lo Blanch (2010), págs. 690-691.

68. Véase Sharp, Walter Gary, *Cyberspace and the Use of Force*, Ageis Research Corp (1999), pág. 140.

se ha realizado previamente la comprobación de que se reúnen las condiciones establecidas hasta aquí, en cuanto a la gravedad del comportamiento inicial, atribución y requisitos de ejercicio de la legítima defensa.

Por otra parte, un estudio del Instituto de Estudios estratégicos se hacía eco recientemente del anuncio del Gobierno surcoreano de su plan de reclutar y formar «a estudiantes hackers como agentes informáticos para combatir las frecuentes amenazas de seguridad cibernéticas» [69]. Contrataciones que, según el mismo documento, defiende John Arquilla, al afirmar que Estados Unidos «en lugar de perseguir a los piratas informáticos de élite, debería reclutarlos para lanzar ataques cibernéticos contra los terroristas islamistas y otros enemigos» [70], en un claro alarde de materialización de la legítima defensa preventiva.

En todo caso, no debemos distorsionar la legítima defensa, que es una categoría jurídicamente determinada, con el propósito de flexibilizarla a las necesidades puntuales de cada momento y Estado, aunque sus promotores sean quienes cuentan con una gran influencia en el orden internacional y se muestran dispuestos a adaptar sus características a las preferencias del momento. Esto no quiere decir que no puedan utilizarse todos los medios precisos para defenderse de un ataque informático grave, sino que han de emplearse exclusivamente aquellos que tengan cabida cumpliendo las condiciones jurídicamente establecidas al efecto. En otro caso, sabido es que la ausencia de proporcionalidad en la defensa es susceptible de generar responsabilidad internacional por el exceso.

69. Véase Caro Bejarano, M. J., «Dilema: formar y reclutar hackers?», *Instituto Español de Estudios Estratégicos*, núm. 56 (2012).

70. No en vano John Arquilla fue asesor del General Schwarzkof durante la primera Guerra del Golfo y asesor del Secretario de Defensa de Estados Unidos durante la ocupación de Iraq de 2003 y en la actualidad es profesor de análisis de la defensa de la Escuela Naval de Postgrado de los Estados Unidos en Monterey, California. Estas manifestaciones las realizó en una entrevista concedida a *The Guardian* el 10 de julio de 2012 y que puede leerse en http://www.guardian.co.uk/technology/2012/jul/10/us-master-hackers-al-qaida

Conclusiones

El tan predicado anonimato que proporciona internet permite a aquellos que cuentan con conocimientos o habilidades suficientes atacar sistemas informáticos ajenos sin identificar al autor del daño que el malware (o badware) provoca. Sin embargo, aunque encontremos a quien (o quienes) lanza el virus difícilmente encontraremos las pruebas precisas para determinar si actúan por cuenta y bajo la dirección de un Estado (o de una Organización Internacional), a pesar de que el establecimiento de esta relación es imprescindible para poder atribuir los comportamientos a un sujeto de Derecho internacional.

En relación a la atribución de los hechos cometidos a un Estado, a pesar de la evolución producida y la emergencia de entes no estatales en la escena internacional, el ordenamiento actual no nos permite reconocer acciones ejecutivas extraterritoriales de los Estados en defensa de sus intereses sin violar la soberanía territorial del Estado en el que pudiera desplegarse. Quizá este tipo de amenazas evidencia la insuficiencia del Derecho Internacional actual para enfrentarlas, debido a la inexistencia de categorías particulares que las ampare.

A pesar de lo anterior, no me parece que estemos en el punto de diseñar nuevas sanciones o nuevos tribunales especiales para juzgar a los ciberdelincuentes internacionales, como propone Sharon R. Stevens [71]. Aunque pudiera ser necesario comenzar a pensar en ello, resulta un elemento muy ambicioso para que pueda prosperar a corto o medio plazo. En principio, podría plantearse su incorporación en un eventual futuro tratado a celebrar en este punto que resulta muy conveniente, pues necesitamos tipificar las acciones que, realizándose con el soporte de internet, consideramos dentro del alcance del concepto «uso de la fuerza», lo que supone en definitiva la utilización de la red como arma de guerra [72].

71. Véase Stevens, Sharon R., «Internet War Crimes Tribunals and …», *loc. cit.*, *supra* nota núm. 4, pág. 657 y ss.

72. Un debate de gran interés sobre la conveniencia de realizar un Tratado Internacional en la materia puede leerse en Hollis, Duncan, «Should There Be An International Treaty On Cyberwarfare?»: http://www2.law.temple.edu/wordpress/blog/2012/06/13/should-there-be-an-international-treaty-on-cy-

Resulta evidente que otros comportamientos, como el espionaje pueden provocar daños y no precisamente leves, en función de cuál sea el contexto, pero dado que carecen de finalidad destructiva no nos plantearíamos su consideración como uso de la fuerza si no fuera por el instrumento utilizado en este caso, debiendo en consecuencia permanecer al margen de él también ahora.

En relación a esta necesidad de regulación, debemos ser conscientes de las dificultades que derivan de la codificación de normas mediante tratados internacionales y más aún del desarrollo progresivo de este ordenamiento: en primer lugar, la lentitud de su elaboración; y, en segundo término, debido al relativismo característico de las normas convencionales. La lentitud en su elaboración responde al segmento temporal que transcurre entre el inicio de la negociación y la entrada en vigor, en ocasiones decenios [73]. Debido al tema que pretendemos regular, el transcurso del tiempo actúa en contra de las necesidades de los negociadores, pues cabe la posibilidad de que, con la elevada rapidez a la que avanza la técnica, cuando el tratado entre en vigor responda a las inquietudes pretéritas, del momento en el que se negoció, pero no de las actuales cuando sus disposiciones pasen a ser jurídicamente exigibles.

---

berwarfare/ y en *Global Security Forum 2012: Fighting a Cyber War del Center for Strategic and International Studies* (CSIS), en http://csis.org/event/global-security-forum-2012-fighting-cyber-war.

73. Existen múltiples ejemplos de esta situación, pensemos por ejemplo en la Convención de Jamaica sobre el derecho del mar, cuyas negociaciones comenzaron en 1973 y su entrada en vigor se produjo veintiún años más tarde, el 16 de noviembre de 1994. Caso que, lejos de ser un supuesto excepcional, es más frecuente de lo que quisiéramos imaginar, solo hace falta mirar los años transcurridos desde el comienzo de la redacción del Proyecto de artículos de la CDI sobre responsabilidad internacional o la Convención de Viena sobre sucesión de Estados en materia de tratados que ya figuraba en el listado inicial preparado en 1949, como posible materia a estudiar y tras ser adoptada en 1978 entró en vigor casi dos decenios después o la de sucesión de Estados en materia de bienes, archivos y deudas que, incorporada igualmente en aquella relación, se adoptó en 1983 y continua durmiendo el sueño de los justos a la espera de recibir los instrumentos de ratificación o de adhesión que permitan que la entrada en vigor se produzca.

Por lo que se refiere al relativismo característico de las normas convencionales, precisamos que adquieran la condición de partes en estos tratados aquellos que cobijan o utilizan armas cibernéticas con los efectos que hemos venido indicando. Sin embargo, la experiencia indica que permanecerán al margen de su articulado, aunque sean sus consentimientos los realmente relevantes para que el instrumento resulte eficaz.

Ante este escenario, quizá la elaboración de tratados menos ambiciosos subjetiva o materialmente pudieran ser la clave para obtener buenos resultados, siempre que esos instrumentos estuvieran fundamentados sobre la conciencia de la necesidad de coordinar los esfuerzos para combatir el problema que se intenta regular. Ciertamente, el precio a pagar por los tratados multilaterales con pretensión de universalidad puede reducir el alcance de las obligaciones asumidas por las partes, favoreciendo su modulación mediante reservas u otras cláusulas útiles a estos efectos. Sin embargo, ambos planos (el del tratado multilateral abierto y el de las acciones puntuales de cooperación y coordinación con un ámbito subjetivo más limitado) lejos de ser incompatibles resultan complementarios, pues permiten adquirir compromisos, aunque sean de mínimos, por los Estados con independencia del grado de concienciación que posean al respecto.

Por otra parte, en el seno del Consejo de Europa tenemos el Convenio sobre la ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001, en el que se regulan entre otros comportamientos los ataques a la integridad del sistema, obligando a los Estados partes a adoptar las medidas precisas para tipificar estos comportamientos como delitos en su derecho interno. Sin embargo, es un tratado cuyo propósito es adoptar las bases para la persecución de los distintos tipos delictuales que utilizan soporte informático, como la pornografía infantil, que cuenta con veintidós instrumentos de ratificación o adhesión de Estados principalmente europeos además de Estados Unidos y Japón. Se trata, en consecuencia, de un tratado internacional útil pero insuficiente tanto material como subjetivamente para los propósitos que aquí perseguimos.

Los problemas de atribución de los ciberataques a un Estado nos conducen a otro escenario: el que nos proporciona la relación

asimétrica que se establece entre el autor del daño (en defecto de aquella atribución) y la víctima estatal. Esta asimetría se evidencia por ejemplo en los recientes ataques contra instituciones suecas, entre ellas las fuerzas armadas [74], reivindicados por Anonimus como reacción a la solicitud sueca de extradición de Julian Assange. En estos supuestos, la insuficiencia del Derecho Internacional es evidente y más cuando manejamos instituciones como el uso de la fuerza y la legítima defensa, pensadas para presupuestos fácticos con una caracterización muy distinta de las que ahora nos preocupan. De momento, para proteger nuestras estructuras básicas de estos ataques debemos profundizar en la cooperación y la coordinación de los mecanismos que nos permitan proteger a nuestras infraestructuras básicas de estos comportamientos.

La evolución de los medios electrónicos nos ubica en una situación en la que las categorías jurídicas clásicas muestran sus debilidades, especialmente las relacionadas con el uso de la fuerza. A pesar de lo cual, las tareas interpretativas pueden suponer una solución mejor que la flexibilización de las categorías existentes que pudiera conducirnos a situaciones indeseadas, como que a través de esos *reblandecimientos* se desdibujara el núcleo esencial del concepto en cuestión. Otra alternativa posible y quizá más plausible sería la creación de categorías conceptuales nuevas que pudieran adaptarse a las nuevas necesidades tecnológicas y a las razonables previsiones de evolución, lo que nos conduce de nuevo a los tratados internacionales. Elijamos la posibilidad que más se acomode a nuestros intereses, hemos de buscar la solución en el derecho y no al margen de él y teniendo en cuenta que el principio que prohíbe la amenaza y el uso de la fuerza, como su excepción la legítima defensa, son conquistas que se han producido a lo largo del tiempo. Lo cierto es que, de momento, aquellas categorías nuevas no solo no existen, sino que parecen lejanas en el tiempo, por lo que debemos conformarnos con la aplicación de las existentes aceptando los límites establecidos con carácter general.

74. Véase noticia de 4 de octubre de 2012 difundida por la agencia EFE y publicada, entre otros en: http://www.elmundo.es/elmundo/2012/10/04/navegante/1349337911.html

Afirmar la posibilidad de aplicar la legítima defensa preventiva a los ciberataques nos conduciría a una situación histórica anterior. Permitir sin excepciones o limitaciones la respuesta armada a una potencial amenaza cibernética tiene tal carga de subjetivismo que ampararía un ataque en cualquier momento, pues cada cual es libre de sentirse potencialmente amenazado en circunstancias alejadas de lo que desde una perspectiva objetiva puede considerarse amenaza. Por otro lado, nos conduciría a un mundo necesariamente menos seguro, puesto que de prosperar resultaría tan lícita para nosotros como para nuestros enemigos reales o virtuales y actuales o potenciales.

La vuelta a situaciones en las que se habla de «guerra justa» lejos de avanzar supone un retroceso a los esquemas anteriores a la Segunda Guerra Mundial con los resultados que conocemos. Por tanto, partiendo de los elementos actuales deberíamos esforzarnos por regular de un modo relativamente rápido pero razonable y razonado el potencial bélico que supone internet. No hacerlo parece una irresponsabilidad y un elemento que permite la quiebra de la seguridad internacional que tanto preocupa a algunos. Evidentemente, la ausencia de reglas concretas beneficia a quienes solo las desean para limitar la capacidad de acción de los demás sin pretender someterse a ellas, pero eso no implica que debamos vulnerar el derecho en respuesta, sino lo contrario. El derecho es nuestro instrumento y aliado, su utilización marca la línea que separa a quienes lo respetan de los infractores. Sinceramente, yo me siento más segura entre los primeros, porque el fin no justifica los medios, máxime si estos últimos vulneran el ordenamiento jurídico establecido en aras a un subjetivismo difícilmente comprobable.

CIBERESPACIO Y BIOSEGURIDAD

Maria Ángeles Cuadrado Ruiz [*]

A mi hermano Antonio (q.d.e.p)

Introducción

Voy a tratar de transmitir, principalmente, tres conceptos: la bioseguridad referida a la biosecurity (no tanto a la biosafety) —aunque en español se utiliza el mismo término para ambas—, qué es la biología sintética y quiénes son los biohackers.

Es evidente que tras los atentados terroristas a las torres gemelas en Nueva York, hace ahora 11 años, el 11 de septiembre de 2001, y seguidamente los envíos de ántrax en octubre de ese mismo año y los posteriores atentandos en Madrid el 11 de marzo de 2004 y en Londres en julio de 2007, nuestra percepción de la seguridad y de si estamos o no seguros ha cambiado.

Asimismo las armas de destrucción masiva, que en el argot militar se conocen como NBQR, (armas nucleares, biológicas, químicas y radiológicas). En realidad la destrucción masiva (de personas, animales o medio ambiente) es lo que tienen en común todas ellas, aunque su naturaleza es muy diferente y las consecuencias que provocan también podría ser distinta. El cine ha llevado a la gran pantalla películas en donde el miedo, el pánico y la amenaza se crean con armas nucleares como por ejemplo, en *Pánico nuclear*, mediante armas químicas, como en *La Roca*, o por armas biológicas, como en *Estallido* o *Contagio*. La amenaza de la radioactividad la hemos visto por televisión tras el accidente de la Central de Fukushima provocado tras un tsunami [1] ¿Y entre

[*] M.ª Ángeles Cuadrado Ruiz, es Profesora Titular de Derecho Penal de la Universidad de Granada.

1. Actualmente también se habla de armas sísmicas como aquéllas que son capaces de provocar terremotos, huracanes, tsunamis, etc.

todas estas armas, las armas biológicas [2] son las armas más difíciles de detectar y su diseminación y utilización puede ocasionar miles de víctimas. Ya que de lo que estamos hablando es de virus, bacterias o toxinas producidas o diseminadas con fines hostiles o no pacíficos. Por ello, constituyen una de las grandes amenazas de nuestra era. Y más aún si agentes incontrolados como son los grupos terroristas consiguen acceder a ellas y utilizarlas.

Los grandes avances de los últimos años en biología molecular ingeniería genética, y biotecnología, junto con las constantes innovaciones tecnológicas en el ámbito informático y de las telecomunicaciones confluyen en el tema de la Bioseguridad y el Ciberespacio.

En el ámbito informático también se habla de «virus» informáticos que envenenan e infectan la red. Muchas de sus variantes se distribuyen rápidamente en mensajes de correo electrónico, propagándose a gran velocidad e infectando cientos de ordenadores o dispositivos móviles.

Por todo ello, y ante el potencial riesgo de que las infecciones continúen produciéndose, se declara el estado de alerta de virus. Lo que significa que en cualquier momento el sistema informático puede contagiarse de algún virus.

Se da por tanto esa similitud de lenguaje y de propagación de los virus en el ámbito informático y la propagación de enfermedades mediante la utilización de los agentes biológicos (bacterias y virus) y toxinas, con fines hostiles, ocasionando graves enfermedades y dolencias que actualmente es, también una amenaza a la seguridad, a la salud pública y al medio ambiente.

La bioseguridad como parte de la seguridad

Evidentemente la Bioseguridad forma parte de esa Seguridad, como estrategia europea e internacional. La Estrategia Española de Seguridad (EES) aborda, por primera vez en nuestro país [3] y de manera integral, los retos para su seguridad. En ella se alude evi-

2. Cfr. y vid. ampliamente Cuadrado Ruiz, M.ª Ángeles, *Las armas biológicas. Aspectos legales,* Granada, 2011.

3. Aprobada por el Consejo de Ministros el 24 de junio de 2011.

dentemente a la ciberseguridad, y también, cómo no, a las armas de destrucción masiva.

«La relación entre seguridad y libertad» [4] no solamente suena como un tema respetable de la filosofía política, sino que lo es, como señala la máxima atribuida a Aristóteles, que quien prefiere la seguridad a la libertad, sería un esclavo. Pero este tema después del «9/11» se ha convertido en un asunto político.

¿Cuáles son, entonces, las preguntas debatidas? Yo les lanzo algunas, para que reflexionen y se cuestionen. ¿Cuánta seguridad necesitamos y para qué la necesitamos? ¿Para nuestra supervivencia, para el Estado vigente, para el Estado legítimo, el Estado de Derecho, el Estado liberal y democrático?, ¿para la libertad? ¿Cuánta libertad necesitamos para ello? ¿Qué «pérdidas» en la libertad son aceptadas a cambio de qué «ganancias» en favor de la seguridad? [5]

Si la disyuntiva entre seguridad y libertad se inclinaba en épocas pasadas hacia la libertad, hoy, basta pensar, por ejemplo en los múltiples controles que tenemos que sufrir para embarcar en cualquier aeropuerto de una ciudad occidental: Quítese el cinturón, las botas, te cachean, no puedes llevar agua, ni crema de cacahuetes… Todas estas rutinas que limitan nuestra libertad, y son ejemplo banales, pero que estamos dispuestos a soportar, ya casi de manera ritual, en aras de una mayor seguridad. ¿Cuánta seguridad necesitamos y para qué la necesitamos?

Acerca de la biología sintética

Si la revolución industrial cambió la vida en el siglo XIX y XX, no me cabe duda alguna de que la revolución tecnológica del siglo XXI viene de la mano de la Biología sintética [6], a la que

4. Vid al respecto, Prittwitz, C., «La desigual competencia entre seguridad y libertad», revistas@iustel.com.

5. Vid., Prittwitz, C., «La desigual competencia entre seguridad y libertad», revistas@iustel.com.

6. «Biología Sintética 3.0» es el nombre del congreso científico internacional, con sede en Zurich, que se celebró del 24 al 27 de junio de 2007 para discutir los recientes avances en la biología sintética. El primero de ellos tuvo lugar en 2005. Vid. Grupo ETC Boletín de prensa, 26 de junio de 2007. Life un-

trataremos de aproximarnos a continuación, y sobre todo de lo que serán sus aplicaciones prácticas, en un futuro nada lejano.

El término Biología sintética [7], fue acuñado a comienzos del siglo XX por el químico francés Stéphane Leduc, La Biologie Synthétique, 1912, aunque hasta 2005 no fue reutilizado para abarcar las conexiones de la Biología molecular y la ingeniería, utilizando un lenguaje importado de los circuitos eléctricos y los sistemas mecánicos de producciones prácticas.

La Biología sintética es un ámbito relativamente nuevo de investigación, que los avances en ingeniería genética han propiciado. La Biología sintética va mucho más allá de las técnicas de ingeniería genética, que han quedado desfasadas, y que fueron usadas anteriormente para producir alimentos y fármacos transgénicos, entre otras aplicaciones.

El objetivo de la Biología sintética es crear una disciplina autonóma respecto de la Biotecnología. ¿Y en qué consiste? Se trata de la «creación» de nuevas formas de vida artificial que, como las máquinas, puedan «construirse» para realizar determinadas funciones [8].

La Biología sintética es, en realidad, un área intedisciplinar que incluye a químicos, biólogos, ingenieros, físicos e informáticos científicos. La «synbio», como la denominan en el argot de los laboratorios —por el acrónimo en inglés de synthetic biology—, se inspira en la convergencia de biología, informática e ingeniería en la escala nanométrica. Es decir, usando un ordenador, secuencias genéticas públicas y ADN sintético obtenido por correo, se tendría el potencial para «construir» o «reconstruir» genes o genomas completos (incluidos algunos patógenos letales) [9]. Esto es, por consiguiente, en lo que consiste la

---

der (re)construction» es el nombre del Simposio que reunió en Viena del 13 al 14 de noviembre del 2008 a científicos de la Biología sintética. www.vbc-phd-symposium.at

7. Vid. al respecto De Lorenzo/ Danchin, «Synthetic biology: discovering new worlds and new words», en EMBO reports vol 9, n 9, 2008, pág. 822 y ss.

8. http://www.ekah.admin.ch/it/temi/biologia-sintetica/index.html

9. ETC Group. Extreme Genetic Engineering, ETC Group Releases Report in Synthetic Biology. Enero, 2007.

Biología sintética. El primer Congreso científico de esta materia tuvo lugar en 2005. Y en Europa, se reunieron por primera vez en Zurich en 2007.

Una aproximación consensuada por un grupo de expertos europeos define la Biología sintética como la ingeniería de la Biología, la síntesis de sistemas biológicos complejos, que exhiben funciones que antes no existían en la naturaleza.

Esta ingeniería puede aplicarse a todas las jerarquías de estructuras biológicas, desde moléculas hasta células completas e incluso a organismos. Es decir, la Biología sintética es capaz de diseñar «sistemas biológicos» de manera sistemática. Es una «ingeniería» y realiza «la síntesis de nuevas funciones». En su aspecto extremo es una ingeniería que necesita «piezas estandars que puedan unirse, utilizando para ello la bioinformática, simulando herramientas que construyan circuitos en los que puedan ensamblarse o modificarse funciones biológicas»

Por tanto, sólo aquellos proyectos que usen partes estandarizadas (genes, proteinas, circuitos…) podrían considerarse propiamente en el ámbito de la Biología sintética [10]. Knight impulsó el concepto de BioBricks (bioladrillos), piezas estandarizadas de ADN que producen proteínas concretas y que se combinan entre sí como en un juego de construcción para customizar una bacteria capaz de emitir luz o detectar arsénico en el agua. Knight anticipó una revolución: «Es la tecnología que va a dirigir el nuevo siglo». Y todo según la filosofía 2.0, de libre acceso y en código abierto.

Es decir, el nuevo campo de la ingeniería genética extrema lo que intenta construir son formas de vida sintéticas (mediante química) y ensamblarlas en el laboratorio para producir «máquinas vivas» —organismos totalmente programados para desempeñar tareas particulares—. Traslandándonos al cine de ciencia «ficción» podríamos pensar en ejemplos como Frankestein o más recientemente Terminator.

10. Serrano, L., «Synthetic biology: promises and challenges», en Molecular System Biology 3:158, 2007, 1.

Los avances en síntesis [11] y secuenciación [12] se han comparado a los de la leyes de la microelectrónica, de tal modo que lo que se intenta es convertir la Biología en una verdadera ingeniería [13], aunque no son sólo los ingenieros sino también otros investigadores de las ciencias fundamentales los implicados en la Biología sintética [14].

No obstante, la complejidad de la vida nos sigue sorprendiendo. Parece que no es tan simple como coger una lista estandarizada cuyas propiedades se han caracterizado cuantitativamente (aminoácidos, bases, genes, proteinas, células…) y unirlas con herramientas de bioinformática para obtener una nueva función biológica. No podemos olvidar que al «unir» partes que se habían caracterizado aisladamente o en otros contextos pueden aparecer nuevas propiedades inesperadas.

Y esa es la incógnita y ese es el riesgo. Si los BioBricks funcionan, puede haber una explosión de aplicaciones, no sólo lo que quieren las multinacionales, sino lo que quiera la gente, como en el software libre. Habrá productos útiles, juguetes y materiales peligrosos. El mundo será más complejo. Y China será clave [15].

Esta nueva disciplina se encuentra en su más tierna infancia. Aunque hasta el momento se ha trabajado más en lo que se

11. El increíble desarrollo de las tecnologías de síntesis de ADN han propiciado que actualmente sea más económico sintetizar un gen que clonarlo. Vid. Bügl, H., y otros DNA «Synhtesis and biological security», en Nat Biotechnol 25, 2007, pág. 627-629.

12. La empresa Pacific Biosciences, www.pacificbiosciences.com 2008, ofrece «un nuevo paradigma para el análisis completo del genoma». Se trata de una máquina que identifica las cadenas de ADN y las secuencia a gran velocidad, lo que «acelera la carrera por conseguir poderosas curas». Pretende así reducir a tres horas los tres años que se tardaba en desentrañar el genoma de un ser humano.

13. Schmidt, M., «Diffusión of synthetic biology. A chanllenge to biosafety». Springer, 2008, pág. 2.

14. De Lorenzo/ Danchin, «Synthetic biology: discovering new worlds and new words», en EMBO reports vol 9, n9, 2008, pág. 822 y ss.

15. Schmidt, M.; Kelle, A.; Ganguli-Mitra, A.; De Vriend, H. (Eds.) *Synthetic Biology the technoscience and its societal consequences,* 2009, VIII, 186, Hardcover ISBN: 978-90-481-2677-4.

denomina Ciencia básica que en las aplicaciones de la Biología sintética, esto puede cambiar rápidamente.

Hoy en día es posible sintetizar ex novo un pequeño virus, reemplazar el genoma de una bacteria por otra o incluso construir grandes trozos de ADN para elaborar circuitos genéticos. Se dispone actualmente de las herramientas de sowtware necesarias para llevar a cabo estas operaciones y en los próximos años, es muy probable que todas estas técnicas se mejorarán considerablemente. El 20 de mayo de 2010 la Revista Science publicaba la obtención de la primera célula sintética [16]. Y, ya se ha podido rediseñar o construir por completo células, bacterias o virus [17].

Los promotores de la Biología sintética dicen que de ella derivarán tremendos beneficios sociales como, por ejemplo, nuevos fármacos para combatir enfermedades como la malaria [18] y nuevas fuentes de energía, como los biocarburantes. De este modo, la estandarización de partes biológicas harán más fácil y atractiva el diseño de nuevos y útiles organismos. Lo cierto es que las futuras aplicaciones se hallan en una fase experimental.

También se ha especulado con que la Biología sintética serviría para luchar contra el cambio climático [19]. Algunos de estos organismos serían diseñados, por ejemplo, para liberarse al ambiente porque producirían etanol o hidrógeno baratos.

Hoy en día la Biología sintética despierta grandes esperanzas. La humanidad se beneficiaría de múltiples formas si las actuales investigaciones lograran fabricar medicamentos o vacunas que salven vidas humanas y aumentasen la producción de alimentos en las zonas empobrecidas del mundo, por ejemplo. Pero también el posible desarrollo de agentes biológicos étnica o racialmente específicos; la propagación secreta de agentes biológicos, a fin de

16. Craig, Science, Rev 20 may 2010.

17. Cfr. Serrano, L., «Synthetic biology: promises and challenges», en Molecular System Biology 3:158, 2007, pág. 2-3.

18. Vid. al respecto RO, DK., y otros, «Production of the antimalarialdrug precursor artemisinic aid in engineerd yeast», en Nature 440, 2006, pág. 940-943.

19. Cases/De Lorenzo, «Genetically modified organisms for the environment: stories of success and failure and what we have learned from them», en International Microbiology (2005) 8:213-222.

alterar las poblaciones destinatarias, o para atacar la infraestructura agrícola o industrial podrían causar males insospechados.

Como ocurrió en tiempos pasados con la energía nuclear, el uso perverso de los agentes biológicos y sintéticos como arma de destrucción masiva podría ocasionar desastres hasta ahora inimaginables. Por todo ello, este caótico y peligroso escenario necesita, a mi modo de ver, de una regulación jurídica y ética que permita a los científicos y a la población en general, actuar dentro de unos márgenes de seguridad.

Porque, «ese mismo microbio mínimo que se podría utilizar para luchar contra el cambio climático podría ser el punto de partida para fabricar un virulento patógeno que puede amenazar gravemente a la gente y al planeta». Esto supondría «una gran alarma» debido a las implicaciones que tiene para la guerra biológica. Pero además, tampoco se han discutido los muchos riesgos socioeconómicos, riesgos para para la salud y el medioambiente, más allá del bioterrorismo [20] que puede propiciar.

Para algunos, los organismos vivos sintéticos se promueven como solución «verde» al cambio climático [21] y, al mismo tiempo, para distraer la preocupación de que pueden usarse como armas biológicas [22].

Así es, la biología sintética ha permido a los científicos en 2005 [23] reconstruir el virus de la gripe española de 1918, que mató entre 50 y 100 millones de personas. Actualmente, no obstante, se sigue trabajando en dicho virus, en principio para obtener una vacuna, pero ¿podrían también utilizarse con fines no pacíficos?

20. Maurer, Stephen M. y otros, «From Understanding to Action: Community-Based Options for Improving Safety and Security in Synthetic Biology,» en Goldman School of Public Policy, University of California at Berkeley, disponible en Internet: http://syntheticbiology.org/Documents.html.

21. Calero Díaz, S., «Nanomateriales en la remediación del cambio climático: recuperación de CO2 y almacenamiento de hidrógeno», conferencia pronunciada en el Aula de Ciencia y Tecnología, de la Universidad de Granada, el 7 de octubre de 2008.

22. En Boletín de prensa Grupo ETC, de 7 de junio de 2007, según opiniones de Jin Thomas y Silvia Ribeiro.

23. Kaiser, J., Resurrected influenza virus yields secrets of deadly 1918 pandemic, en Science, 2005 (310), pág. 28-29.

En septiembre de 2008 fue exhumado el cuerpo de un aristócrata británico que murió como consecuencia de la gripe española, hacía más de 90 años [24]. Todo ello forma parte de un estudio destinado a combatir futuras pandemias de gripe. Sir Mark Sykes, propietario de tierras de Yorkshire (norte de Inglaterra) murió en Francia en 1919 a causa de la pandemia de 'gripe española' que afectó al mundo entre 1918 y 1919 ¿Por qué fue exhumado? Los expertos creen que su ADN podía encerrar la clave para hallar una cura de esta enfermedad. Los expertos, que a principios de 2007 anunciaron su intención de exhumar el cadáver de Sykes, confíaban en que el particular ataúd de plomo hubiese permitido conservar el virus de la 'gripe española', cuyo ADN puede tener una estructura genética similar a la de la variante de la gripe aviar. La cepa que provocó la pandemia del principios del siglo XX es la H1N1, similar a la responsable de la epidemia que azota hoy en día a las aves (H5N1). H1N1, que originalmente atacaba también a los alados, mutó para convertirse en un virus letal para los seres humanos. Sólo existen cinco muestras útiles del virus H1N1 en todo el mundo y ninguna procedía de un cuerpo bien preservado por un ataud de plomo. El H1N1 ya había sido secuenciado por científicos utilizando muestras congeladas encontradas en Alaska, pero muchas cuestiones permanecían sin resolver como, por ejemplo, cómo el virus mata a sus víctimas y la forma en que mutó en el año 1918». Por eso se exhumó. Y qué casualidad al año siguiente se desata la gripe porcina, luego denominada gripe A…

Los investigadores trabajan, asimismo, con partes de microorganismos responsables del ébola, el dengue, la viruela, el Nilo Occidental y otros patógenos.

Predecir el resultado de nuevas combinaciones o reconstrucciones de ADN será imposible, pero podría llevar a la creación organismos patógenos completamente nuevos (pensemos en la gripe porcina o la gripe A) que sean atractivos para quienes los pretendan utilizar con fines hostiles. Muchos gobiernos ya prohíben la producción o exportación de ciertos patógenos, pero

24. Vid. *El Mundo*, 17 de septiembre de 2008.

también es cierto que mediante la Biología sintética éstos podrían producirse, comprarse y rediseñarse pieza por pieza sin causar sospecha alguna [25].

Es por lo que hay gran preocupación de que patógenos peligrosos, como el virus de la viruela o el Ébola, u otros, puedan «re-construirse» en los laboratorios y usarse como armas biológicas.

De la destrucción de la vida se pasa a su fabricación. Es lo que Michael Foucault denominaba bio-poder: ya no es matar, sino conferir la vida de parte a parte, lo que podría conducir a «una apuesta eugenésica de la sociedad» [26].

Por otro lado, esta accesibilidad a la Biología sintética también podría, asimismo, provocar cambios sin precedentes respecto a la seguridad.

Cada vez son muchas las personas, y en un futuro no muy lejano, aún más, las que sin una tradicional formación en Biología o en Genética, e incluso sin estudios universitarios, serán capaces de producir sistemas biológicos y llevar a cabo las «re-construcciones biológicas», las «máquinas vivas» para las aplicaciones civiles o defensivas. En este sentido, la Biología sintética podría, asimismo, fomentar una nueva cultura de hackers, los «biohackers» que podrían «re-construir» nuevas formas de vida, produciendo sintéticamente sustancias ilícitas y mucho más baratas [27], al margen de todo tipo de supervisión o control. La facilidad para construir nuevos sitemas biológicos o nuevas formas de vida, consecuentemente, crea también, por consiguiente, mayores riesgos en seguridad y los accidentes y las actuaciones por imprudencia o negligencia, sin duda alguna, se multiplicarán.

25. Maurer, Stephen M., y otros, «From Understanding to Action: Community-Based Options for Improving Safety and Security in Synthetic Biology,» en Goldman School of Public Policy, University of California at Berkeley, disponible en Internet: http://syntheticbiology.org/Documents.html.

26. Cfr. Foucault, M., *La volonté de savoir*, 1970.

27. Schmidt, M., «Diffusión of synthetic biology. A chanllenge to biosafety», Springer 2008, pág 1 y ss.

Los Biohackers [28]

La biología sintética ha hibridado con una media naranja, la informática, para alumbrar uno de los fenómenos más curiosos e interesantes de los últimos años: los biohackers, biotecnólogos con el sueño prometeico de robar a la naturaleza el secreto de la vida y a los centros de investigación el poder para manejarla, crear organismos hasta en un garaje y que todo ello sea abierto, compartido y público; vida 2.0. o 3.0. [29]

Si los hackers, son los piratas de la informática, los biohackers son los piratas de la genética, son los piratas del ADN, que también conforman un «gremio», actúan organizados y desafían con sus experimentos a los grandes laboratorios.

¿Y qué hacen los biohackers? Pues modifican células, fabrican transgénicos (aunque esto es la la prehistoria en comparación con la Biología sintética), duplican cadenas de ADN… y lo hacen… en su casa o en su garaje.

¿Y los biohackers son biólogos, genetistas o conocedores de las Ciencias de la vida? Probablemente la mayoría no.

Internet lo que ha hecho es hacer accesible el acceso al saber. Y por ejemplo, el código del genoma humano está disponible en un fichero de 1,44 gigaoctetos (el tamaño de una película pirateada).

¿Cúal es el reto? ¿Cómo minimizar lor riesgos?

Habrá que vigilar al biólogo amateur, entrenarlo en bioseguridad y alejarlo del material peligroso, estableciendo códigos éticos y dándole a conocer las prohibiciones de los tratados internacionales como la Convención de armas biológicas ratificados por España, así como las conductas tipificadas como delitos relacionadas con estos ámbitos. Pienso que constituiría una buena estrategia para la prevención penal general y especial y para promover la concienciación de un uso lícito de las nuevas tecnologías, en la aplicación de las ciencias de la vida.

28. Cfr. Yanes, J., BIOhackers: reventar y reinventar la biología desde los garajes, Madrid 18/12/2008, en ABC.

29. Idem.

Les propongo un experimento para que hagan en casa. Los ingredientes son: tomen un poco de su saliva, una pizca de sal, una gota de líquido lavavajillas, de zumo de pomelo, y un dedo de ron.

Al cabo de unos instantes dos filamentos blanquecinos deben aparecer en la superficie. Se puede sacar con un palillo de dientes. Ese es su ADN.

¿Qué ha sucedido? El detergente rompe la pared de las células, la sal se amalgama con el ADN, el pomelo neutraliza las proteínas que podrían perjudícarlo y el alcohol lo persigue hacia la superficie [30]. Para un biólogo esto es un experimento banal, pero para los biohackers tiene un sentido pedagógico.

Para los que piensan en la ingeniería genética como algo casi mágico, o de laboratorios ultrasofisticados, ver su propio ADN con ingredientes tan familiares rompe muchas barreras. Puede que en un tiempo no muy lejano el Biohacking se convierta en un hobby planetario… ¿Libertad frente a seguridad? a un subjetivismo difícilmente comprobable.

30. Cfr. Yanes, J., BIOhackers: reventar y reinventar la biología desde los garajes, Madrid 18/12/2008, en ABC.

Parte III

TECNOLOGÍAS DE IMPARABLE PROGRESIÓN EN EL CIBERESPACIO. INVESTIGACIÓN, PREPARACIÓN Y RETOS EN MATERIA DE CIBERDEFENSA MILITAR

CONCIENCIACIÓN SOBRE LA EXPANSIÓN Y VULNERABILIDADES DE LOS DISPOSITIVOS MÓVILES

Daniel Ruiz Betelu [*]

Introducción

¿Estamos seguros con nuestros smartphones, tablets, etc.? Esta es la pregunta que tratábamos de responder dentro de las jornadas del curso de verano sobre ciber seguridad organizadas por el Centro Mixto UGR-MADOC.

Como anticipo de las conclusiones y como ya veremos durante la exposición del presente documento, la respuesta es no. No porque no estén disponibles las herramientas, o capacidades técnicas que hacen posible que la respuesta sea la contraria, sino que, ya sea por desconocimiento, por falta de información, o por simple dejadez, no usamos todos los recursos a nuestro alcance para mantener nuestros terminales seguros. ¿A qué es debido esto? Pues principalmente y aunque es importante el desconocimiento que tenemos de estos nuevos sistemas, ya citado anteriormente, creo que la causa primera es una falta grave de concienciación.

Para hacernos una idea de conjunto de lo que significa esta falta de concienciación durante la conferencia se aportaron una serie de datos y cifras. A fecha de hoy esas cifras han aumentado y siguen creciendo de manera exponencial.

Los dispositivos móviles

Por ejemplo, el número de teléfonos inteligentes —*smartphones*— ha llegado a la cifra de mil millones de unidades este trimestre, todo ello según las cuentas de la empresa de análisis Strategy

[*] Daniel Ruiz Betelu, es Director de I+D de Voice Consulting, S.L. Madrid.

Analytics. Es decir, uno de cada 7 habitantes del planeta tiene un teléfono inteligente.

Marca que se consigue 16 años después de que se lanzara el primer móvil inteligente, además, y según la predicción de futuro de la misma fuente, se llegarán a los 2.000 millones en 2015, tan solo tres años después.

La intrahistoria nos muestra como durante estos 16 años, la industria de los dispositivos móviles ha cambiado de manera drástica. Nokia, fabricante líder durante años, dejó su puesto en favor de una empresa de ordenadores, Apple, que en 2007 decidió sacar un móvil con pantalla táctil, el iPhone. Otros fabricantes como Samsung, HTC, etc. que junto a la aparición de un nuevo sistema operativo para móviles, Android, se apuntaron a esta nueva revolución.

Por centrarnos a un nivel más cercano, en el mercado español, un reciente estudio revela que los —smartphones— son ya mayoría. El 60% de los teléfonos móviles renovados en España en el trimestre de diciembre a febrero de 2012 son «inteligentes» es decir, uno de cada tres móviles que hay en el mercado.

He aquí, que ante la dimensión que están tomando estas cifras en cuanto al número de terminales que hay en estos momentos y el que habrá en un futuro próximo que un factor muy importante sea el de la seguridad, teniendo en cuenta además, que son dispositivos con un valor de información altísimo. Correo electrónico, documentos, agendas, contactos, fotos, videos, música, etc. todo ello fácil de portar y además, rápidamente accesible.

Sistemas operativos comunes

Es importante por tanto, dentro de la difícil tarea de hacer estos dispositivos más seguros, conocer los nuevos sistemas operativos que utilizan estos terminales inteligentes. Sistemas como iOS, Android y Windows Phone son las nuevas piezas clave dentro de este engranaje de la tecnología móvil y es imprescindible conocerlos, saber hasta donde alcanza su uso y cuales son sus principales problemas o vulnerabilidades. Algunas cifras del alcance de su uso aparecen a continuación.

El sistema operativo Android ha extendido su dominio en Europa y especialmente en España, donde arrasa con el 87% de

cuota de mercado. El sistema operativo de Apple, IOS representa el 3% del mercado español, Black Berry el 7,2 por ciento y Symbian, el sistema operativo de Nokia, el 3,4 por ciento en este mes de junio de 2012. Cierra la lista el sistema operativo de Windows, con sólo el 2% de los smartphones renovados en España en el último trimestre.

Esta tendencia indica que la mayoría de los móviles vendidos en España en lo que va de 2012 son Android, dejando muy atrás a Symbian, RIM o iOS, y que además es la única plataforma que crece, ya que el resto de sistemas operativos ve reducida su presencia. Hay casos muy llamativos como el de Symbian cuyas ventas el año anterior reflejaban un considerable 55%.

La tendencia no sólo es española. Lo mismo sucede en EEUU, el principal mercado de teléfonos inteligentes del mundo. Allí, ya más de la mitad de los smartphones vendidos llevan Android, aunque sin cifras tan radicales.

Según el último panel de comScore, los terminales Android superaron por primera vez la barrera del 50% de terminales vendidos. En febrero, el 50,1% de los smartphones llevaban el sistema operativo de Google, lo que supone haber ganado un 17% extra respecto a febrero de 2011.

Los números de comScore dejan en segundo lugar al iOS de Apple, que ha subido hasta el 30,2%. Por su parte Black Berry y Windows Phone siguen perdiendo posiciones. La firma canadiense se queda en el 13,4%, y los móviles con el sistema operativo de Microsoft apenas llegan al 3,9%. Allí, Symbian apenas tiene presencia. Lo que nos deja en un mundo de sistemas operativos móviles con dos contendientes principales.

De lo que ya no hay ninguna duda es que el crecimiento o la popularidad de los llamados dispositivos móviles inteligentes, smartphones o tablets, sigue en aumento y que además la plataforma o sistema operativo con mayor tasa de crecimiento es Android, que es una de las plataformas más amenazadas junto con Facebook.

El porqué de su popularidad es claro y se explica en que la mayoría de estos equipos, gracias a los nuevos sistemas operativos, nos permite llevar encima una pequeña computadora con todo nuestro mundo controlable con total comodidad.

Vulnerabilidades

También explica el hecho de que los programadores de virus cada vez prestan más atención a las plataformas móviles, buscando vulnerar los dispositivos y acceder a nuestros datos privados, y en consecuencia, que las principales plataformas amenazadas sean sistemas que tienen que ver con estos dispositivos.

Las estafas, el 'malware' y el robo de datos se han trasladado de los entornos que actualmente eran los más amenazados como las webs, al territorio de las redes sociales, los 'smartphones' y las 'tablets', que se han convertido en el nuevo punto de interés de troyanos, 'spammers' y aplicaciones maliciosas.

Según publican diferentes empresas de seguridad en sus informes semestrales, como por ejemplo Bit-defender, los mercados de aplicaciones para dispositivos móviles están experimentando el mayor aumento de robo de datos, estafas y 'malware' hasta la fecha, en especial para aplicaciones basadas en Android. Bitdefender apunta que una de cada cuatro aplicaciones de Android es maliciosa y buscan el robo de datos, la estafa o el 'phishing'.

Por su parte Kaspersky, una de las empresas más reconocidas en el sector, cifra en 15.000 los archivos maliciosos que se interceptaron en el último trimestre, a lo largo del uso estándar del 'smartphone'. Lo que supone tres veces más que el trimestre anterior del año.

F-Secure, otra compañía de seguridad, en este caso finlandesa, ha realizado por su parte otro estudio en el que calcula que el crecimiento de —malware— ha sufrido un incremento del 64% respecto al trimestre pasado.

Y por último, según Sophos, otra empresa con renombre en el sector, y tomando como referencia su propio informe, explica que este año pasado tuvimos un aumento de más del 150% en casos de malware en las plataformas móviles, y concretamente, más de un 3000% en lo que a Android se refiere.

No hay que hacer excesivos cálculos en cuanto a que el crecimiento de 'malware' es y será abrumadoramente grande, teniendo en cuenta que, entre todos los abonados a los smartphones este año, según cálculos, nos descargaremos unas 40.000 millones de aplicaciones.

En cuanto a cifras por países España es el cuarto país del mundo en sufrir esta recepción de archivos maliciosos basados en el sistema operativo de Android, después del Reino Unido, Francia y China, por orden decreciente.

Aun cuando algunos de estos datos son excesivamente alarmistas, si que es cierto que la plataforma móvil Android es una de las que más ha crecido en los últimos años, no en vano, ya hay más de 500 millones de dispositivos activos y la cifra sigue creciendo. Y este crecimiento va asociado a que usuarios malintencionados y spammers tomen como objetivo los smartphones Android, vía exploits, aplicaciones infectadas, troyanos, etc.

El sentido común es la mejor seguridad

El problema principalmente radica en que, un mayor uso de las funcionalidades de un 'smartphone', no conlleva una mayor protección contra virus y 'malware'. Situación que es aprovechada por usuarios malintencionados.

Al final, de lo que no hay duda y no hay que olvidar es que el malware está presente en Android, en mayor o menor medida, pero que la mayoría de las veces, solo hay que tener sentido común y junto con mantener algún que otro protocolo de seguridad, no tener que preocuparnos nunca por estas amenazas, ya que en la mayoría de las ocasiones somos los propios usuarios que recibimos este tipo de archivos los que no somos conscientes de que estamos siendo espiados, robados, estafados o que hay terceros que tienen acceso a los datos almacenados en nuestro 'smartphone' o 'tablet' como información bancaria, direcciones o redes de contactos.

Hemos visto ya que las amenazas son reales, existen, que hay muchos datos que lo confirman y que desde luego van a ir a más. Pero cuáles son esas amenazas y cómo podemos defendernos...

Las principales amenazas que pueden sufrir nuestros dispositivos móviles se pueden establecer en diferentes categorías.

Ataques basados en web y redes. Estos son lanzados desde sitios web maliciosos o incluso por sitios legítimos que han sido comprometidos. En este caso el sitio malicioso se aprovecha del navegador de nuestro dispositivo e intenta instalar malware o robar los posibles datos confidenciales que fluyen a través del propio navegador.

Malware. En esta categoría se incluyen los virus computacionales tradicionales, gusanos, y caballos de Troya.

Ataques de ingeniería social. Consiste en engañar a los usuarios de modo que estos, revelen datos sensibles o instalen algún malware. Se suelen realizar mediante phising y ataques dirigidos.

Abuso de recursos. Buscan que se realice un mal uso de la red, del dispositivo o los recursos. Se utilizan técnicas como el SPAM o los ataques de negación de servicio.

Amenaza a la integridad de los datos. Intentar dañar o modificar de alguna manera los datos buscando por ejemplo, interrumpir las operaciones de una empresa.

Pérdida de datos. Pérdida que hace que un usuario con o sin motivos maliciosos acceda a información sensible del dispositivo. Esta es la principal amenaza que existe hoy en día.

Sabiendo que un alto porcentaje de las veces que un malware llega a cualquier sistema es por responsabilidad del propio usuario que, bien sea por desconocimiento o porque ha sido victima de un buen truco de ingeniería social, termina instalando aplicaciones peligrosas, es conveniente conocer algunas pautas a seguir para mejorar la seguridad de nuestros dispositivos y que nuestra convivencia con estas nuevas tecnologías no nos deje un sabor de boca amargo.

Algunas recomendaciones de utilidad

Son trece, las claves que nos ayudarán a mantener nuestro dispositivo siempre seguro.

*En el sector empresarial es conveniente la utilización de aplicaciones de administración, configuración y gestión de dispositivos de manera centralizada***.** Los usuarios de dispositivos Android e iOS sincronizan regularmente sus equipos con servicios de cómputo en la nube de terceros (calendarios, documentos) y con sus computadoras de escritorio domésticas. Esto puede exponer eventualmente datos comerciales sensibles almacenados en estos dispositivos a sistemas que están fuera del control de la compañía. Con sistemas de gestión centralizados esto se evitaría.

No liberar los dispositivos móviles. Los dispositivos «liberados» («jailbroken, root»), o aquellos cuya seguridad ha sido deshabilitada, son un blanco atractivo para los atacantes ya que disponen de todos los permisos y accesos abiertos al mismo.

Verificar la lista de permisos que solicita cada aplicación. ¿Cuántos de nosotros miramos los permisos de las aplicaciones antes de instalarlas? Cada una de las aplicaciones, al momento de ser instaladas, solicita permisos para acceder a determinadas funciones del dispositivo y algunos de nuestros datos. Cuando instalamos debemos estar muy atentos a que los permisos solicitados por la aplicación sean coherentes con el propósito de la misma. Por ejemplo: algo normal sería que una aplicación para recomendar eventos que se van a producir cercanos a nuestra ubicación nos pida acceso al GPS, mientras que un simple juego de cartas que nos pida acceso a toda nuestra libreta de contactos y el contenido de nuestros mensajes de texto debería despertar sospechas. Además, si concedemos a una aplicación permisos de súper usuario es muy importante que sepamos que es de fiar. Existen aplicaciones como LBE o Pdroid que nos permiten gestionar estos permisos de usuario individualmente bloqueando aquellos que no se crean necesarios.

Instalar aplicaciones directamente desde las tiendas oficiales. Aunque se han visto afectadas en algún momento, son el medio más seguro para obtener aplicaciones. No es seguro utilizar tiendas de aplicaciones alternativas, así como descargar los archivos .apk o .ipa desde fuentes no confiables para realizar la instalación manualmente. Al no haber sido sometidas a un control por parte de los canales oficiales de distribución, estas aplicaciones podrían haber sido alteradas para funcionar de manera distinta o instalar otras aplicaciones no deseadas que podrían comprometer nuestra seguridad y privacidad.

Es importante mantenerse alerta sobre lo que instalamos en nuestros terminales, la opción de permitir la instalación desde fuentes desconocidas es un arma de doble filo, es recomendable extremar la precaución ante aplicaciones móviles ya que muchas fuentes «sospechosas» que ofrecen gratuitamente software de pago, podrían venir con troyanos o malware integrado.

Instalar una aplicación antivirus y mantenerlo actualizado. Muchos de los antivirus más populares para equipos ya se encuentran disponibles para las plataformas móviles, la mayoría gratuitas y de gran rendimiento. Adicionalmente, muchas de estas aplicaciones, ofrecen funcionalidades extra como opciones de back-up, recu-

peración, rastreo y borrado remoto en caso de pérdida o robo. También es necesario **r***ealizar análisis periódicos* para verificar la seguridad. Se pueden probar distintas alternativas fiables. Aplicaciones como Sophos, Avast, AVG, Norton, etc. nos permiten una seguridad continua al comprobar en su base de datos cada vez que vamos a instalar una aplicación, y así asegurarnos de que no está infectada. Este consejo se hace aún más necesario en caso de hacer uso de aplicaciones que no hemos descargado desde los cauces oficiales.

Instalar una aplicación de seguridad para el rastreo, recuperación y borrado remoto en caso de pérdida o robo. La mayoría de los antivirus actuales para dispositivos móviles llevan capacidades extras como las citadas. Avast, Sophos, AVG son antivirus con sistemas de seguridad en caso de pérdida o robo, pero también Prey, Cerberus, Comodo o LookOut son aplicaciones sencillas que nos permiten hacer de nuestro dispositivo un elemento más seguro. Aunque algunas de estas aplicaciones son sistemas de localización de tu terminal en caso de pérdida, Plan B o Where's my Droid, otras de las citadas anteriormente no sólo te permiten localizar tu terminal, sino también borrar su contenido de manera remota.

Hay que tener en cuenta que hoy en día los terminales móviles no sólo tienen un precio más que considerable, sino que si los perdemos estamos perdiendo también un objeto con cientos de direcciones de correo, teléfonos y datos personales sobre nosotros y nuestros contactos. Para evitar que esta información caiga en malas manos, es conveniente hacer dos cosas. La primera, cuidar siempre nuestro smartphone o tablet (procurando no olvidarlo en cualquier sitio).

La segunda, instalar una aplicación de rastreo y localización, por si lo extraviamos o algo peor.

Introducir un control de acceso, patrón o contraseña de bloqueo del dispositivo. Aunque ya hemos visto que en algunos casos es posible saltarse este sistema de seguridad, es un sistema altamente fiable manteniendo además algunas otras precauciones. De esta manera evitamos que una persona que coja tu teléfono pueda acceder al contenido, agenda, etc.

Android permite el acceso a archivos vía USB siempre y cuando esté activa la opción *USB Debugging / Depuración USB.* Por ello es recomendable que cifres todos los datos del terminal con la op-

ción integrada del sistema operativo de Google dentro de Ajustes —> Seguridad. Este proceso tarda la primera vez y requiere cerca de una hora. Existen algunos métodos que permiten saltarse este sistema de seguridad, que requieren que el modo de depuración en el móvil se encuentre activado. Es importante mantener desactivado este modo cuando no se utilice.

Usar aplicaciones de cifrado de datos. Tanto en nuestras comunicaciones como en el almacenamiento de datos. Utilizar aplicaciones alternativas o complementarias con sistemas de cifrado más seguros a otras en que la seguridad es muy pobre. Hay alternativas más seguras a muchas de las aplicaciones más utilizadas en alguno de los campos como pueden ser la mensajería instantánea o almacenamiento en la nube. Spotbros, Glyph o Prot-On para mensajería instantánea y en el caso de almacenamiento en la nube, existen muchas muy seguras como Box, Google Drive o incluso Boxcriptor que funciona como complemento al propio Dropbox, la aplicación reina en este campo.

Mantener la mínima información posible en nuestro smartphone. Nada de guardar contraseñas o detalles de la tarjeta de crédito en archivos sin cifrar. Tampoco contraseñas a la hora de navegar por nuestro dispositivo móvil, en caso de ser necesario guardar las contraseñas es preferible usar una solución segura y cifrada como por ejemplo LastPass.

Realiza copias de seguridad del dispositivo, restaurándolo a valores de fábrica en caso de que tengamos que entregarlo para una reparación o para otra causa que requiera que el dispositivo esté durante un tiempo en otras manos distintas a las nuestras.

Desactivar las conexiones Bluetooth, NFC y Wi-Fi en caso de no utilizarlas, siempre es mejor prevenir que curar una infección por un exploit inalámbrico. No activar Bluetooth si no es necesario o en caso de que lo fuera, no dejar el dispositivo reconocible. De la misma forma no activar NFC si no se va a utilizar y si es necesario no perder de vista nuestro dispositivo.

Las tecnologías de comunicación como Bluetooth o NFC han demostrado ser muy vulnerables. Por ejemplo, Bluetooth es particularmente vulnerable a datos de entrada incorrectos. Éstos pueden causar que la operación del dispositivo Bluetooth sea lenta, muestre un comportamiento inusual o falle completamente.

En el peor de los casos, las entradas incorrectas de datos pueden ser usadas por un atacante externo para obtener acceso no autorizado al dispositivo Bluetooth.

También recientemente se ha demostrado que se puede tomar el control de los 'smartphones', gracias a una vulnerabilidad de la tecnología Near Field Communication (NFC). El ataque funciona poniendo el teléfono a pocos centímetros de distancia de un chip —de un cuarto de tamaño— o situándolo de tal manera que toque con otro dispositivo NFC.

Mediante una etiqueta NFC, por ejemplo, que tocase nuestro teléfono, se puede hacer que el navegador web, sin que el dueño haga nada, abra una URL maliciosa. La funcionalidad que, por el momento, tienen las etiquetas NFC es la misma que cuando se escanean códigos QR, pero de forma más sencilla, ya que solo hay que acercar el móvil al TAG para que lo lea. Con los accesos desde los QR-CODE sucede exactamente lo mismo pudiendo establecer una URL maliciosa como destino del mismo.

Mantener nuestro dispositivo actualizado. Los fabricantes y desarrolladores de aplicaciones realizan actualizaciones de su software con nuevas funcionalidades pero también con parches para la corrección de fallas de seguridad por lo que se recomienda mantener actualizado tu smartphone.

Actualiza el firmware a la última versión. Cada día aparecen nuevas vulnerabilidades en las aplicaciones que nos descargamos y usamos. En aplicaciones muy utilizadas como WhatsApp a nivel de mensajería instantánea, y Dropbox a nivel de almacenamiento en la nube, se han descubierto recientes fallas de seguridad que permitían el acceso a nuestros mensajes y a nuestra información almacenada. En estos casos es necesario instalar las correspondientes actualizaciones en cuanto estas estén disponibles, y en caso de que la aparición de estas actualizaciones se retrase, es recomendable utilizar aplicaciones alternativas a las que contienen vulnerabilidades.

Verificar la URL, y el certificado en caso de navegación segura sobre conexiones HTTPS a través de nuestro smartphone o tablet. Este consejo se hace extensible a navegar desde cualquier dispositivo, sea móvil o no.

No realizar tareas delicadas (conexión a bancos, mensajes privados, etc.) sobre WIFIs abiertas de las que desconozcamos su procedencia.

Blindarse en redes inalámbricas con cortafuegos como DroidWall o utilizar programas VPN que cifran todos los contenidos como WiTopia, Relakks o IPredator es la mejor manera de movernos en estos entornos.

Tampoco es recomendable utilizar sistemas o aplicaciones de voz sobre IP móvil dentro de estas redes, ya que la señal de voz que se transmite en una comunicación entre dos terminales móviles, viaja a través de Internet empleando un protocolo IP y es posible, tratándose de instalaciones VoIP no seguras, la captura de paquetes VoIP (emisión de voz en paquetes IP) y la extracción de conversaciones contenidas en este tipo de conexiones.

Conclusiones

Como conclusión a esta exposición hemos visto que los datos están ahí. Que en esta rápida carrera tecnológica no hay marcha atrás, y que lo único que nos falta es precisamente el objeto de esta parte del curso sobre ciber seguridad, el concienciarnos. Concienciarnos sobre estos dispositivos, sobre como los utilizamos y sobre lo que guardamos en ellos, concienciarnos de que las tecnologías avanzan a pasos agigantados, para bien y para mal, y concienciarnos además, de que hay usuarios con oscuras intenciones que intentarán aprovechar los fallos de las propias tecnologías o nuestros posibles descuidos, para buscar su propio beneficio.

Pero lo que también debemos conocer es que existen soluciones. Soluciones que posibilitan que estemos seguros, protegidos, con nuestros dispositivos móviles, y que no tengamos que preocuparnos más de estas amenazas.

El problema es que para el usuario medio, en el uso de los 'smartphones', 'tablets' y demás dispositivos móviles, la seguridad de momento, no ocupa la importancia que debería. Como pasa en muchos otros temas, la sociedad toma conciencia y ve la verdadera dimensión de un problema demasiado tarde, cuando el daño ya está hecho y no hay solución.

CIBERDEFENSA MILITAR Y CIBERGUERRA EN EL CONTEXTO DE LA SEGURIDAD GLOBAL

Fernando Gordo García [*]

Introducción

Transcurría el convulso año de 1942 en el que el mundo estaba sumido en una atroz Segunda Guerra Mundial sucesora de una primera en poco menos de treinta años, cuando Norbert Wiener, un matemático estadounidense, introduciría por primera vez la «Cibernética», entendiéndola tal y como ha llegado hasta hoy día. Dicho término derivado del griego «*kibernete*», designa al timonel, a quien pilota o dirige una nave. De él derivan también otras palabras como gobierno o gobernante, y desde entonces la diferencia entre dos palabras con el sufijo «ciber», —las cuales se han prodigado popular e ilimitadamente en los últimos años—, no resulta ser otra que la resultante de comparar ambas palabras prescindiendo del recurrido sufijo. Es decir, salvo por el contexto del sufijo, encontraremos las mismas diferencias o similitudes entre ciberataque y ciberdefensa, que entre ataque y defensa.

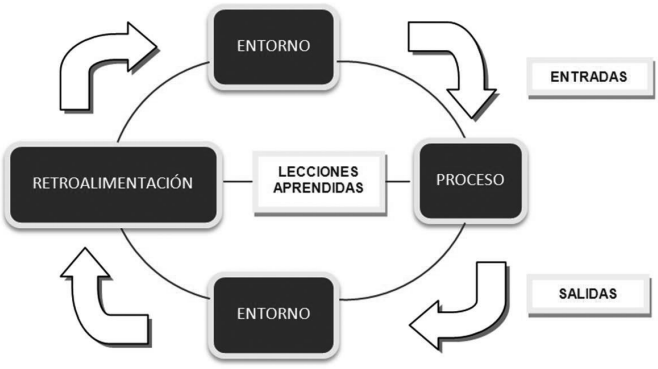
A Wiener su país le encomendó la gran responsabilidad de dar solución al problema urgente de poder derribar los veloces cazas enemigos con los cañones antiaéreos de la época. Ni los reflejos humanos más notables servían ya para disparar contra blancos con movimientos tan rápidos, y el matemático pronto comprendió que indiscutiblemente se tenía que conceder esa misión a las máquinas.

Los elementales ordenadores de aquel tiempo no respondían a esa necesidad, precisaban implementar algo innovador. Fue en-

[*] Fernando Gordo García, es Comandante de Ingenieros, Transmisiones, de la Dirección de Investigación, Doctrina, Orgánica y Materiales del MADOC en Granada.

tonces, cuando un inadvertido principio que se había empleado anteriormente en telecomunicaciones —con el tubo en vacío y el control de volumen automático de las radios—, ofreció la solución a Wiener. Se trataba de la realimentación —*feedback*—. Años más tarde, en 1948 Wiener publicó definitivamente su obra *Cybernetics*[1], donde quedaban reflejados los principios de aplicación en la regulación y control de todo tipo de máquinas y, por ende, de todos los sistemas dinámicos y sus procesos. Wiener no sólo se refería a los procesos mecánicos de ingenios artificiales, también hablaba de los animales, personas y todo tipo de organismos vivos y procesos sociales. Consideraba la «transformación» gracias al aprendizaje y por tanto a las lecciones aprendidas tan recurridas hoy en muchos campos, como la unidad formal básica de la Cibernética, siendo la innovación el catalizador y mejor «motor del cambio», para progresar y en definitiva para mejorar.

Figura 1. Las lecciones aprendidas y la realimentación en los procesos



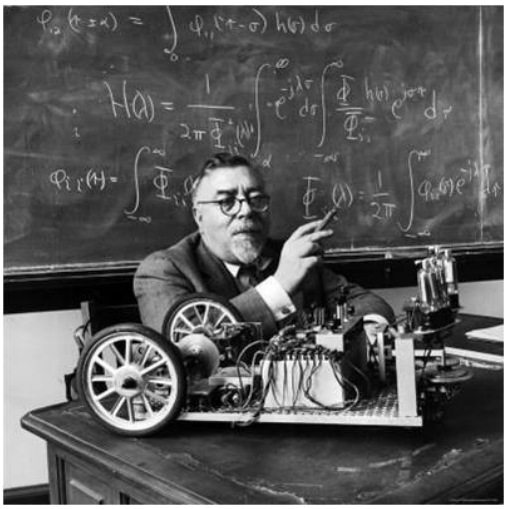
Hemos rebasado desde entonces una primera década de un siglo XXI en un mundo multipolar repleto de amenazas y conflictos asimétricos; delincuencia organizada, terrorismo, flujos

1 Norbert Wiener, *Cybernetics; or, Control and Communication in the Animal and the Machine*. Cambridge, Mass: Technology Press, 1948.

migratorios, estados fallidos, corrupción en muchas de sus dimensiones políticas y económicas…que han conducido y catalizado de alguna forma al actual periodo de crisis. Excelentemente enmarcado en su contexto global de la seguridad por el primero de los autores de este libro, —el profesor Roldán—, el mundo al que nos referimos está sin duda actualmente determinado al mismo tiempo por la inmediatez y disponibilidad de la información que facilita todo tipo de transacciones económicas, la libertad de movimientos y mercancías, la transferencia de conocimientos, de ideas e incluso de sentimientos de alguna forma.

Todo ello, está evolucionando tan velozmente que cada día se hace más necesario regular su empleo de una forma flexible, responsable y segura. A tal fin, la Cibernética puede ayudar sin duda porque en definitiva no se trata más que de un método elemental de análisis que facilita la aplicación de las lecciones aprendidas, el aprendizaje y por tanto, la mejor toma de decisiones.

Figura 2. Norbert Wiener en 1948 publicó su obra Cybernetics



El empleo de la Cibernética con propiedades de sistemas determinados puede aproximarse también, como argumentaba Wiener, al realizar el análisis de sistemas no determinados, es decir, de comportamientos sociales no aleatorios que podrían describirse

estadísticamente. No nos faltan lamentablemente ejemplos recientes de todo ello a los que acudir en cualquier parte del mundo, particularmente en el ámbito de la Política y de la Economía donde similares desafortunadas actuaciones de sus líderes, a menudo frecuentes, conducen a situaciones que repercuten de forma negativa en la vida de los ciudadanos sin llegar éstos a comprender cómo se originan. Preguntas como: ¿Qué influye sobre los líderes políticos al adoptar sus decisiones? ¿Cuáles pueden ser las consecuencias entre las demandas sociales y las respuestas a las mismas de esos líderes? ¿Qué medidas preventivas pueden y deben tomar los gobernantes en determinados momentos? ¿De qué mecanismos legales, reales y asequibles, pueden disponer las poblaciones para resolver y sancionar los graves errores de sus líderes políticos y económicos?

Evidentemente la Cibernética puede favorecer a alcanzar respuestas que ayuden a cambiar las propias pautas de las organizaciones y sus objetivos finales en beneficio global de las sociedades aplicando las lecciones aprendidas y progresando al fin y al cabo. Gracias en parte a la facilidad y accesibilidad a la información y al conocimiento, éstas en su conjunto, afortunadamente hoy día, ven así aceleradas la innovación y su aprendizaje acortando la brecha, al menos en este sentido, con la clase social de «timoneles» que las gobiernan y que deben representarlas responsablemente en su totalidad teniendo en cuenta sus necesidades e intereses vitales. Siendo positivos como es nuestra obligación, pensemos que las crisis son entradas negativas en el proceso de realimentación visto, las cuales también lo enriquecerán aprendiendo también de aquello que no es tolerable en los sucesivos procesos para poder progresar.

Admitida la escasez presupuestaria actual que afecta indudablemente de forma importante a los presupuestos destinados a la seguridad y la defensa, la última Directiva de Defensa Nacional Española de julio de 2012, enfatizaba ya la necesidad de asegurar en estos momentos críticos una España fuerte y unida para mantener la influencia necesaria en el contexto internacional que vele por sus intereses. Refiere en este sentido que es necesaria una Política de Defensa responsable y coordinada de todos los instrumentos en manos de los distintos departamentos, manteniendo unas capacidades y un nivel de disuasión creíble y suficiente. En línea con nuestra argumentación anterior, esta política considera clave la participación

ciudadana como única fórmula válida que tiene en sus manos la continuidad y profundidad suficiente para velar por nuestros intereses; la independencia, la soberanía, la integridad territorial, la paz, la libertad y la propia prosperidad de todos los españoles. Gran relevancia concede a la disuasión como resultado de disponer de unas capacidades junto con la determinación de usarlas llegado el caso. La mayor garantía de paz y seguridad es la credibilidad sin duda alguna.

Sin embargo, debemos apuntar en este punto algo acerca del carácter disuasorio de las capacidades de ciberdefensa. En este caso no se ajustaría a las actividades tradicionales de demostración de poderío o supremacía respecto a otros, puesto que nos encontramos ante la dificultad de identificar los objetivos reales contra los que se debería actuar. Por tanto, se hace esencial antes de llevar a cabo cualquier actuación disuasoria, valorar de forma inteligente y balancear previamente la cantidad de información que se pone a disposición de aquellos potenciales adversarios, en contraste con el deseo disuasorio que se pretenda obtener. Será necesario tener muy presente pues, que una vez realizada tal demostración de hegemonía en el ciberespacio, —donde la asimetría y el anonimato son dos de sus principales vulnerabilidades y oportunidades al mismo tiempo—, muy probablemente y desde ese preciso momento, perderá en buena medida la pretendida efectividad disuasoria. En otras palabras, habremos mostrado al enemigo nuestras capacidades [2].

Tanto la reciente Estrategia Nacional de Seguridad de 2013 como diferentes documentos sobre seguridad nacionales, instan convergentemente a impulsar de forma decidida la gestión integral de la ciberseguridad en el marco de los principios que establezca la necesaria Estrategia de Ciberseguridad Nacional, en la que se deben encontrar reflejados todos aquellos que por sus responsabilidades o tareas profesionales e incluso personales, utilicen el ciberespacio. En este dominio global y común, las Tecnologías de la Información y de las Comunicaciones —TIC—,

2. Las denominadas vulnerabilidades de Zero-Day se refieren precisamente a aquellas que no son en general conocidas por la gente ni las empresas siquiera, y constituyen un potencial de ataque importante en reserva

tienen su inagotable e imparable campo de actuación. Como se apuntaba al principio al hablar de la Cibernética, en realidad, empleadas con responsabilidad, las TIC no son más que herramientas que nos ayudan en nuestros propios procesos de toma de decisiones, no sólo en el trabajo diario, también en las propias relaciones sociales para constituirnos en los verdaderos timoneles —kibernetes— que gobiernen nuestras vidas de acuerdo con nuestras expectativas de paz, seguridad y prosperidad [3].

Ciberespacio, ciberseguridad y conflictos armados

Si realizamos un análisis comparativo de distintas estrategias nacionales de seguridad como EEUU, Reino unido, Francia ó la última de España, continuaremos encontrando elementos análogos relacionados con las principales amenazas o focos de conflictividad actuales que se presentan en diversas combinaciones. Todos, constituyen importantes amenazas a la seguridad, y por tanto, pueden ser fuentes de conflictos armados. El Ciberespacio aparece como denominador común en todas esas amenazas. Conforma un nuevo dominio global y común de grandes oportunidades para la prosperidad de las naciones, pero también para la actuación de quienes pretendan actuar en contra de los principios de la democracia, justicia y libertad de las mismas.

El Jefe de Estado Mayor de la Defensa, hablaba en junio de 2013 de las tres prioridades necesarias ante los retos de Seguridad y Defensa del siglo XXI: la inteligencia, la ciberdefensa y los equipos de fuerzas especiales. Consideraba a las Fuerzas Armadas del futuro, como actores protagonistas que se enfrentarán a situaciones complejas, en las que igual se pueden enfrentar a misiles que a piratas y para ello junto con la creación de los mandos de Ciberdefensa, de Operaciones Especiales, de Vigilancia Aérea y Marítima, se iniciaba una transformación que aspira a consolidar las bases de la estructura operativa del futuro centrada en una Fuerza Conjunta Operativa versátil, resiliente y con capacidad «expedicionaria».

3. Extractado del artículo del mismo autor: *Kybernetes de nuestra prosperidad*, columna de Opinión del diario impreso de información general «Ideal» de fecha 19 de septiembre de 2012.

Fuerza que deberá actuar en un complejo entorno operativo donde el rasgo principal actual es «la incertidumbre», que requiere un planeamiento que recoja, como una capacidad esencial, poder «reaccionar a tiempo». Concluía el JEMAD que por ello, es necesario potenciar la inteligencia y los sistemas de mando y control para conseguir «velocidad del mando», ya que la posibilidad de tomar decisiones en el menor tiempo posible «da ventaja» a un ejército sobre otro. «Hace falta actuar de forma decisiva, rápida y efectiva» y resaltaba algunos de los riesgos actuales, que se encuentran en el arco Irán-Mauritania, donde confluye la posibilidad de un Irán nuclear con la expansión del yihadismo y las ideas antioccidentales; en la zona del Golfo de Guinea, un vasto espacio en el que se mueven con impunidad bandas de crimen organizado; y la zona del Asia Pacífico, donde hay varios puntos conflictivos en Corea del Norte o China aparte de otros riesgos como los biológicos y el cambio climático.

Consecuencia de ello, las operaciones militares de las Fuerzas Terrestres se desarrollarán dentro de conflictos armados entre poblaciones locales con culturas desconocidas, la mayoría de las veces en medio de crisis humanitarias con posibles limpiezas étnicas o cualquier otro tipo de violaciones de los derechos humanos. Uno de los elementos claves será la interoperatibilidad, no sólo tecnológica sino también en aquellos aspectos humanos necesarios para operar entre coaliciones de ejércitos de otros países y otros actores no sólo militares.

Reconocido el ciberespacio como un dominio de actuación en expansión, cada vez son más los países que elaboran estrategias a nivel nacional sobre ciberseguridad. En ellas se identifican conceptualmente los aspectos clave de lo que se suele denominar de forma imprecisa pero popularmente como «ciberguerra»; tanto en lo referente a la amenaza que representa el uso del ciberespacio, como el de la oportunidad que conlleva su utilización. La estrategia española de ciberseguridad está finalizada, aunque pendiente de publicación en la fecha de la redacción de este trabajo. De su génesis, retos y líneas de acción, se hablará detalladamente en la última parte de este libro. Probablemente será sancionada en breve tras actualizar la estrategia española de seguridad a finales del mes de mayo de 2013, cuando el Consejo de Ministros

aprobaba un informe que incluye la nueva Estrategia de Seguridad Nacional. En dicho documento contempla la creación de un Consejo de Seguridad Nacional que presidirá el Presidente del Gobierno y que cuenta con la presencia de la mitad de los ministros. Este consejo tiene la misión de funcionar como una comisión delegada que debe mantener reuniones periódicas, además de las que sean necesarias en casos extraordinarios, y podrá contar con la presencia del Rey cuando éste lo considere oportuno.

La nueva Estrategia de Seguridad Nacional incorpora una vez más lo que denomina «nuevas amenazas» más allá de las que hasta ahora eran habituales. Entre los doce riesgos de seguridad nacional se incluye el ciberterrorismo, los boicots a suministros energéticos, el espionaje, los ataques a infraestructuras críticas, además de los conflictos armados y el terrorismo.

Complejo entorno operativo de actuación de las fuerzas terrestres. Vectores principales de ataque

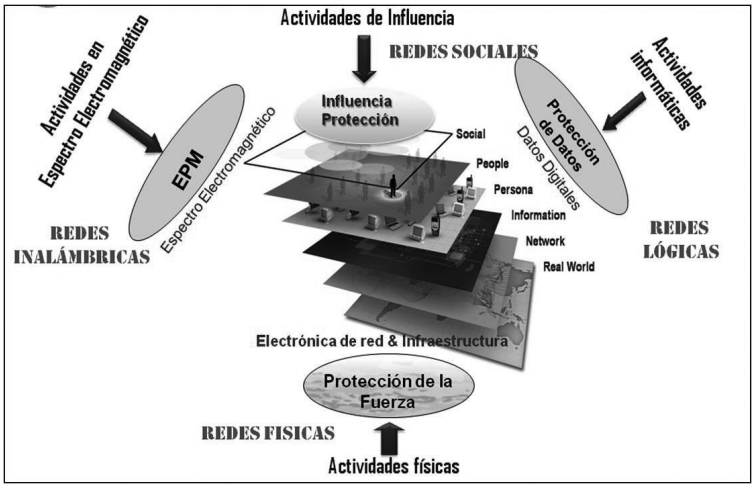
Consecuentes con la importancia de este nuevo escenario de seguridad, nuestra Doctrina de empleo de las Fuerzas Terrestres [4] de 2011 denominaba anticipadamente al Ciberespacio, en consonancia como: «Entorno virtual resultante de interconectar un conjunto de sistemas de información, a través de todo tipo de redes e infraestructuras físicas, y los usuarios con los que interactúan, todo ello con independencia de su ubicación geográfica». Paralelamente al inicio de cualquier investigación ulterior sobre dicho entorno, —una de las misiones del MADOC en apoyo a la preparación—, resulta clave el conocimiento y la disponibilidad de las tecnologías incorporadas a los medios de las unidades y a las tácticas, técnicas y procedimientos de combate. Sirva como ejemplo decir, que para la definición de muchos conceptos reflejados en esta última edición de la Doctrina, se tuvieron muy en cuenta no sólo las lecciones aprendidas provenientes de distintas zonas de operaciones, sino también todos los trabajos de la serie de Experimentos Multinacionales en los que el MADOC viene participando desde 2008, en

4. Doctrina de Empleo de las Fuerzas Terrestres. Mando de Adiestramiento y Doctrina. Granada. 2011.

particular, los relativos a *Cultural Awareness* y a *Cyberspace*, MNE-6 y MNE-7.

Tal es la importancia que está alcanzando el uso del Ciberespacio en las operaciones, que se expondrán a continuación algunos ejemplos de los principales vectores de ataque a los que se enfrentan; bien mediante actividades en las redes físicas e infraestructuras, actividades en el espectro electromagnético en las redes inalámbricas, actividades en los datos en las redes lógicas, ó mediante actividades de influencia y gestión de la percepción en las redes sociales.

Figura 3. Vectores de ataque a las distintas capas del ciberespacio



Quizás el ejemplo más recurrido y significativo lo encontramos, hasta la fecha, en el año 2007 en Estonia, cuando las páginas oficiales de varios departamentos del Gobierno, bancos y prensa, quedaron bloqueadas totalmente por ciberataques del exterior, con posible origen en Rusia, consistentes en ataques distribuidos de denegación de servicio, DDoS. El detonante del ciberataque se debió a que la estatua conmemorativa de la victoria rusa en la Segunda Guerra Mundial, colocada en el centro de Tallin durante la ocupación soviética, fue trasladada a un cementerio militar. Aunque Estonia solicitó a la OTAN incluso la aplicación del artículo 5, finalmente no se ejecutó si bien expertos en ciberdefensa de la

organización acudieron en su ayuda. A raíz de lo anterior y ante los nuevos temores de una agresión rusa a los países bálticos, surgieron varios debates acerca de los compromisos exigibles a la OTAN sobre la garantía de protección basada en dicho artículo que establece la defensa mutua entre los aliados [5].

Figura 4. Evolución de las iniciativas en Ciberdefensa en el ámbito de la OTAN

De mayor importancia desde el punto de vista de las operaciones militares, fue el conflicto armado entre Georgia y Rusia en el verano del año 2008. Las ciber-operaciones militares evolucionaban acordes con el planeamiento de la maniobra de los combates armados de las fuerzas terrestres, y para ello necesitaban adquirir continuamente Inteligencia. Las ciber-operaciones, cuya atribución tampoco ha sido reconocida por Rusia hasta hoy, fueron conducidas en coordinación con las operaciones armadas y sirvieron para debilitar eficientemente la capacidad de respuesta militar y política de Georgia. Estas se iniciaban con antelación y

5. Véase La OTAN aprobó un plan secreto en defensa de los países bálticos. El País, 07 de diciembre de 2010.

numerosos medios fueron secuencialmente tomando nota puntual de todo ello [6].

Figura 5. Características de las actividades en el Ciberespacio.

Otro ejemplo de actividades de ataque físico, y al mismo tiempo de influencia, es el del soldado analista de inteligencia de EEUU acusado de filtrar a *WikiLeaks* material clasificado. Entre ese material se halla un video en el que se ve cómo un helicóptero estadounidense mata a un grupo de civiles en Iraq donde se encontraban dos periodistas de la agencia Reuters [7]. Es sospechoso además de haber filtrado otros documentos clasificados acerca de las guerras de Afganistán y de Iraq, así como unos cables diplomáticos de las embajadas estadounidenses. Por todo ello, fue acusado oficialmente de «ayudar al enemigo».

Otro caso relacionado con lo anterior y muy significativo, es el de la confidencialidad y «lealtad debida» en este nuevo dominio que constituye el ciberespacio. Nos referimos en particular al extécnico de la CIA y exconsultor de la Agencia Nacional de Inteligencia (NSA) que se responsabilizó de filtrar datos de ciberespionaje en EEUU y que afirmaba lo siguiente a los medios de comunicación:

6. Véase CCN-CERT, *Ciberataque contra el sitio web de la presidencia de Georgia,* 22 de julio de 2008.

7. El vídeo Collateral Murder, es uno de los más difundidos en Internet; http://www.youtube.com/watch?v=Wfzz12LzMuQ

> Tengo la intención de pedir asilo a cualquier país que crea en la libertad de expresión y se oponga a que la privacidad global sea la víctima... permitir que el Gobierno estadounidense intimide a su pueblo con amenazas de represalias por revelar malas acciones es lo opuesto al interés público… las filtraciones han hecho que los estadounidenses ahora entiendan que tienen el poder de decidir por ellos mismo si están dispuestos a ceder su privacidad a un estado de vigilancia constante.

Este ingeniero que trabajó durante cuatro años en la NSA admitió ser el origen de la información revelada [8] por los diarios *The Guardian* y *The Washington Post*, sobre programas de espionaje secreto que permiten consultar a diario registros de llamadas en Estados Unidos y extraer información de servidores de Internet con el objetivo de espiar a extranjeros sospechosos de terrorismo. Las investigaciones por parte de los servicios de Inteligencia Norteamericanos y el Departamento de Justicia determinarán la responsabilidad y posibles consecuencias penales de estos hechos, que afectan seriamente a la lucha antiterrorista.

Las redes sociales y la gestión de la percepción

Otra muestra evidente de actividades de influencia en el ciberespacio, es la que constituyen los movimientos sociales recientes en contra del «statu-quo» en los países del Norte de África. Desde el reciente caso turco hasta el más significativo del caso de Egipto en el que se puso de manifiesto claramente que el intento gubernamental de censurar actividades en el ciberespacio, puede servir de detonante para enardecer más si cabe, a las poblaciones que se manifiestan en contra de injusticias como las dictaduras ancladas al poder y a la corrupción política y económica de décadas. Más revelador resulta aún, si se tiene en cuenta que tan sólo el 20% de la población en Egipto a comienzos de 2011, disponía de algún acceso a Internet y sin embargo lograron derrocar al gobierno.

8. Para ampliar información sobre el PRISMA Data Collection Program, véase: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Expectantes una vez más de movimientos de protesta social catalizados por el fácil acceso a las TIC, como los iniciados en mayo de 2013 en Turquía contra su presidente, no podemos más que seguir alerta en relación con lo que se decía en uno de los artículos de la revista Ejército acerca del caso de Egipto [9].

> …expansión de ideas, sentimientos e información son algunos de los elementos comunes de este continuo trasiego de pensamiento global, transformado ahora de forma inmediata, en ejecución práctica. Las tecnologías libres están permitiendo que el ser humano participe en actividades que hace tan solo unas décadas quedaban a merced del poder de movilización de los partidos políticos, grupos organizados o en ciertos casos, de «personajes ilustres» que por sus hechos han pasado a la historia de la Humanidad. Los sistemas y aplicaciones basados en software libre en los que todo su código fuente puede ser utilizado, modificado y redistribuido por cualquiera dentro de los términos de las licencias libres, están siendo uno de los catalizadores de este «motor de cambio social». Desde el detonante del caso tunecino, siguiendo por Argelia, Egipto, Yemen, Libia, Siria e incluso en cierta medida Marruecos entre otros países, todos han tenido el denominador común de las movilizaciones espontáneas en contra del statu quo. La resignación al orden político establecido ha dado paso al inconformismo para reivindicar la libertad que ofrecen los intereses y derechos normales legítimos de las democracias, contra estructuras cerradas y ancladas en el autoritarismo político y la corrupción…así las TIC, ¿pueden usarse para negar a los gobiernos?, ¿cuándo debe ser un derecho básico la comunicación a través de ellas?, ¿la desconexión sentará un precedente para otros países que imiten a Egipto?, ¿hasta dónde llegan los derechos y deberes en la nube digital? La relevancia actual en materia de ciberseguridad en muchos países engloba las capacidades defensivas y lógicamente ofensivas donde las Fuerzas Terrestres estén preparadas para «combatir», pero: ¿quién y cómo establece el marco legal para actuar?

En cuanto a ejemplos de ataques físicos en el ciberespacio, uno de los más importantes lo encontramos sin duda en el año

9. Véase «Espectadores de otro hito histórico. De los Mamelucos a las redes sociales». *Revista Ejército*, núm. 852, marzo de 2012, págs. 6-13. Madrid. http://www.ejercito.mde.es/Galerias/multimedia/revista-ejercito/2012/R_Ejercito_852.pdf

2010 en Irán. Un sofisticado virus informático, Stuxnet, paralizó totalmente las centrifugadoras de enriquecimiento de uranio, haciéndose con el control del sistema SCADA, encargado de gestionar y procesar los datos de la central nuclear de Natanz, y de muchas infraestructuras críticas del mundo. Su evolución, el virus Flame descubierto en 2012 como una amenaza persistente avanzada, APT, se considera por muchos como la primera «ciberarma» por su gran potencia y complejidad del diseño.

Figura 6. En las revueltas de Turquía de 2013 se han llegado a enviar más de dos millones de tuits en tan sólo ocho horas. (Fuente: AFP. CNN 06 junio 2013)

La importancia de la ciberedefensa en el nivel táctico de las operaciones y la convergencia de las actividades en el espectro electromagnético y el ciberespacio

En el nivel más táctico en ZO, encontramos el claro ejemplo de la amenaza de los artefactos explosivos improvisados —IED—. Con el imparable avance de las tecnologías de información y comunicaciones —TIC—, se puede al mismo tiempo beneficiar la insurgencia siendo capaces de operar en bandas nuevas del Espectro Electromagnético en las que los inhibidores de frecuencia deben adaptarse continuamente. Al mismo tiempo, los avances y grandes posibilidades en los dispositivos móviles del tipo smartphones, en paralelo con el acceso a coberturas radio como

las de tercera generación, 3G, abren nuevas puertas de opciones de ataque a los adversarios en zonas de operaciones. No sólo para la amenaza IED, también para sus actividades de Mando y Control e Inteligencia [10]. Las misiones de Inteligencia para conocer anticipadamente de qué tecnología disponen los insurgentes, y qué tácticas, técnicas y procedimientos utilizan, resultan vitales para la Protección de la Fuerza.

Son muchos los analistas que se esfuerzan, no sin argumentadas razones, en enmarcar las actividades en el ciberespacio sin olvidar conceptos y clasificaciones ya existentes que interaccionan en gran medida, e incluso se solapan en muchas de sus extensiones doctrinales y prácticas. Buena muestra de ellas son las operaciones de información, INFOOP, las operaciones de influencia, las operaciones en red, CNE Computer Network Operations, las actividades de ataque o defensa de las redes CNA, CND, Computer Network Attacks / Defense, ciberseguridad, ciberguerra, ciberdefensa, las recién nombradas en la doctrina Norteamericana como Cyberelectromagnetics operations, y un largo etcétera. Terminología imprecisa que puede provocar cierta ambigüedad e incluso malentendidos procedentes de la inexactitud y falta de acuerdo e incluso del consenso tal y como algún experto analista [11] ha apuntado. De esta forma, un claro ejemplo de esta ambigüedad era mostrada en una de las muchas opiniones reflejadas en Internet que decía: «….*hay que recordar que el ministro Morenés ha llegado a advertir del riesgo de un atentado vía internet contra una central nuclear*», este analista se hacía la pregunta: *¿la protección y consiguiente reacción frente a un potencial ataque a través de Internet contra una instalación de este tipo compete a los responsables de la ciberseguridad, de la ciberdefensa o a ambos a la vez?* Esperemos que la inminente publicación de la Estrategia Nacional de Ciberseguridad en España pueda dar respuesta a la pregunta anterior y lo que es más importante, que se inicien cuanto antes los planes de acción que la pongan en práctica.

10. Actualmente en Afganistán, compañías como MTN con participación Iraní entre otros países, están ampliando este tipo de acceso móvil.

11. Seguridad en el Ciberespacio. Blog de Fernando Dávara. 26 de enero de 2013. http://fernandodavara.com/seguridad-en-el-ciberespacio/

Una vez admitida globalmente la definición del ciberespacio ofrecida por distintas fuentes, —Doctrina de primer nivel para el empleo de las fuerzas terrestres, los conceptos de OTAN, nacionales del EMAD, del Mando Conjunto de Ciberdefensa del Ministerio de Defensa, foros internacionales como el MNE, etc.—, como el conjunto de tecnologías de la información y comunicaciones, que contienen los distintos tipos de redes y tecnologías donde se incluye Internet, diferentes sistemas de información y sensores que lo conforman, hay que resaltar que el elemento clave en todo ello es la información. Por tanto, podríamos simplificar la definición de ciberespacio limitándonos a decir que es el *universo global por donde la información fluye y se almacena.*

El citado Mando Conjunto de Ciberdefensa, en caso de que se produzcan ciberataques, será uno de los responsables principales de actuar en ese nuevo dominio para obtener, analizar y explotar la información de los incidentes y ejercerá «la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional». De esta forma, podrá planear y ejecutar estas acciones relativas en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas y en otras redes y sistemas que se le encomienden, por lo que podemos comprender lo novedoso y trascendental de ello, al no limitarse a la protección de los sistemas de utilización estrictamente militares.

En cuanto al nivel táctico de las operaciones, es oportuno citar los excelentes resultados que ofrecen las unidades de EW tácticas desplegadas actualmente en ZO. Por ello, estas unidades tanto en sus misiones específicas, como en aquellas en coordinación con las de Operaciones Especiales, de Inteligencia o de Reconocimiento, necesitarán de una gran preparación técnica y permanente formación y adiestramiento, para desarrollar acciones que doten a las brigadas orgánicas polivalentes (BOP), de la capacidad de defensa, explotación y respuesta, a su nivel, en Ciberdefensa Táctica.

Son muchas las amenazas, las necesidades, y las grandes oportunidades al mismo tiempo que ofrece el uso apropiado del ciberespacio en las operaciones y misiones a las que se enfrentan la Fuerzas Terrestres desplegadas en una ZO. Valga el «simple» ejemplo de los sistemas de información para Mando y Control, C2IS, o

Inteligencia que se apoyan en la Red Radio de Combate ó en las Redes Satélite. La convergencia con las misiones tradicionales de la EW son evidentes, y por ello algunos países aliados, como se ha citado en el caso de EEUU, hablan de actividades ciber-electromagnéticas [12], si bien se simplifica a menudo usando el concepto de ciberoperaciones [13]. Noticias recientes como la de que un virus informático infectó las cabinas de los UAV norteamericanos Predator impidiéndoles despegar, o que la insurgencia aprovechó la vulnerabilidad de que no se cifraba el vídeo que se transmitía a las tropas en el terreno, han puesto en evidencia y originado fugas de información comprometiendo las operaciones de ejércitos aliados.

Las noticias sobre la trascendencia táctica y operacional, no sólo estratégica, de las «armas cibernéticas» se pueden encontrar con elevada frecuencia en la prensa, no sólo especializada, también de información general. Acudamos a un ejemplo reciente cualquiera. «*Las herramientas portátiles de guerra cibernética*», es el titular [14] de una noticia reciente en la que nos informan acerca de que el Departamento de Defensa de Estados Unidos ha solicitado herramientas para análisis expedito de datos electrónicos de móviles y equipos de almacenamiento de datos y guerra electrónica, EW. Una solicitud que al parecer, y de acuerdo con la fuente, no es nueva. Explica así, que hace cinco años los soldados estadounidenses comenzaron ya a utilizar herramientas similares desarrolladas para la policía, como COPEE (*Computer Online Forensic Extractor*). La herramienta consistía en una lápiz de memoria USB que cuando se capturaba un ordenador enemigo, se insertaba y podían ejecutarse más de cien programas de software para recuperar rápidamente cualquier información que hubiese en el ordenador. COPEE podía revelar rápidamente contraseñas, desencriptar archivos, revelar actividades recientes en Internet y muchas otras

12. Véase FM-3-36. Electronic Warfare. HQ Department Army. EEUU. November 2012. Appendix E. Cyberelectromagnetic activities support to Electronic Warfare.

13. Véase ADP-6.0. Mission Command. HQ Department Army. EEUU. May 2012.

14. Véase El Observatorio. *Revista Atenea* núm. 45.

informaciones que se pueden encontrar en cualquier Backtrack de Linux.

Figura 7. Las «armas cibernéticas» tienen su trascendencia en las operaciones

Evidentemente estas actividades se podrían hacer sin el USB COPEE, pero con ello se facilitaba y aceleraba la obtención de información. Microsoft distribuyó miles de memorias COPEE a la policía y a personal de inteligencia militar en EEUU y a terceros países, según la fuente. COPEE fue desarrollada principalmente para ayudar a las investigaciones relacionadas con actividades criminales en Internet. La inteligencia militar pronto comprendió que resultaba muy útil para detectar rápidamente planes de los enemigos, lo que facilitaba contraatacarlos. Los terroristas utilizan los CIS portátiles y nunca realizan ataques sin contar con ellos. A COPEE, le sucedió un proceso de desarrollo de herramientas para otros aspectos de la «ciberguerra», y el propio COPEE se ha actualizado varias veces, para contrarrestar las herramientas que los hackers han desarrollado a su vez contra la citada herramienta.

Estos instrumentos de análisis, —desarrollados por Microsoft inicialmente para la policía y las fuerzas armadas—, las empleaban

las patrullas militares en Iraq. En definitiva, permiten que alguien sin experiencia previa pueda analizar la actividad de redes inalámbricas en zonas de despliegue y determinar qué objetivos podrían atacarse con armas cibernéticas. Indica la misma referencia que DARPA continúa trabajando en el desarrollo de sistemas similares para guerra electrónica, en especial plataformas aéreas, para no restar tiempo a los pilotos ni a los operadores de sistemas. Para las fuerzas terrestres sin embargo, este tipo de misiones para penetrar o perturbar redes inalámbricas, serían más factibles. Este tipo de «armas» para realizar ciberataques, deben ser lo bastante simples para que un soldado de cualquier arma o especialidad aprenda a manejarlo con una formación mínima, pero lo suficientemente flexibles y potentes para que los operadores CIS o de EW avanzados, puedan explotarlas en toda su extensión para alcanzar el máximo beneficio para las fuerzas propias.

Evitaremos en cualquier caso emplear el término de ciberguerrero, al menos de momento. Si bien se podría admitir el término de ciberguerra por su popularidad y amplia difusión actual, el terreno movedizo desde el punto de vista legal y jurídico en el que todavía se mueven las acciones en el ciberespacio, no debería permitir que cualquier criminal, delincuente, terrorista o simple hacker motivado por la competición o el deseo de actuar como mercenario para obtener dinero, pueda identificarse con un combatiente o un soldado legítimo dotado de valores intrínsecos muy lejos de los anteriores. Un soldado empleará los CIS o la EW en sus acciones reglamentariamente ordenadas en los conflictos en los que así se decida legalmente y por tanto nada tiene que ver con los distintos tipos de activistas ilegales del ciberespacio.

Continuando en el nivel táctico que nos interesa, hay que reconocer que ya se han dado los primero pasos decididos en zonas de operaciones. Buen ejemplo de ello son los principios de la Estrategia de Ciberseguridad del Comandante de la ISAF —*International Security Asistance Force*—, sancionados en 2011, anticipatorios al despliegue generalizado de la actual *Afghan Mission Network* (AMN), red federada de misión que en el caso de España se desplegó incluso hasta el nivel de las COP, —*Combat Outpost*, posiciones avanzadas de tipo Compañía desplegadas en la misión de Afganistán—. Esta fue una de las referencias principales que se

tuvieron muy presentes para desarrollar el complejo e innovador ejercicio de experimentación en Ciberdefensa Militar Táctica, dirigido por el MADOC con el apoyo del ITM en 2012.

En cuanto a la perspectiva actual nacional de la Ciberdefensa, se puede decir que en realidad es una evolución del concepto de INFOSEC, más estático y orientado a la protección, a uno nuevo más operativo y dinámico en el que las FAS deberán adquirir la libertad de acción y seguridad para llevar a cabo con éxito las operaciones militares que incluyen la capacidad de respuesta. Desde el ámbito conjunto, como se ha apuntado anteriormente, se elaboraron los documentos teóricos de la Visión y el Concepto del JEMAD sobre Ciberdefensa Militar en 2011. En el primero, se destaca que la capacidad de Ciberdefensa Militar (CDM), se subdivide en las de Defensa, Explotación y Respuesta, afectando a todos los niveles; estratégico, operacional y táctico. Posteriormente, todo ello se detallaría más en el Concepto. Finalmente la parte práctica está reflejada en el Plan de Acción del JEMAD para implementar la CDM de julio de 2012, donde se asignaban plazos y responsabilidades al nivel conjunto y a los Ejércitos y Armada, en tres fases que constituyen la capacidad básica, intermedia y completa final. Uno de los puntos más significativos, se encuentra en la inclusión de la capacidad de respuesta, es decir, la capacidad ofensiva de realizar ciberataques, elemento clave quizás, templado además posteriormente en la Orden Ministerial de 2013 de creación del Mando Conjunto de Ciberdefensa.

En suma, se podría concluir diciendo que la perspectiva actual nacional de la Ciberdefensa, está basada en realidad en una evolución del concepto de INFOSEC orientado a la protección, hacia uno nuevo más proactivo que incluye la capacidad de respuesta, como principal novedad.

Paso adelante del ET. Investigación del Madoc en ciberdefensa militar

El MADOC a finales de 2011, consecuente con la acelerada dinámica de todo lo expuesto hasta aquí, y consciente de la gran importancia de dominar el Ciberespacio en las misiones de las Fuerzas Terrestres, inició actividades para profundizar sobre otras iniciativas en curso, de carácter general, desarrollando un Progra-

ma de Investigación, PINV. Su parte teórica introductoria, dirigida a la ciberseguridad global, contó con el apoyo de la Universidad de Granada para analizar las implicaciones del Ciberespacio donde el Ejército de Tierra tiene uno de los elementos del entorno operativo de actuación. A la parte teórica, le sucedió como se ha comentado, una experimental e innovadora con los objetivos principales de:

—identificar los riesgos y amenazas para las misiones que desarrolla el Ejército de Tierra en esta denominada quinta dimensión,
—analizar los aspectos técnicos y jurídicos más relevantes que pudieran ser comunes a otras áreas como el ciberterrorismo,
—recomendar acciones de coordinación, estudiar las tendencias del complejo entorno operativo, y experimentar conceptos para detectar carencias operativas recomendando la adaptación, en su caso, de la doctrina, orgánica y los materiales,
—por último, obtener recomendaciones mediante el proceso científico del desarrollo de conceptos y su posterior experimentación, tanto en forma de Lecciones Aprendidas como de Buenas Prácticas, que sean válidas para todas las unidades de la Fuerza Terrestre, y difundidas en forma de manuales o guías rápidas de empleo.

Las acciones realizadas en el ciberespacio buscarán paralizar, colapsar, corromper o destruir los flujos de información militares o civiles, alterando tanto el desarrollo de una operación militar como condicionando el normal funcionamiento de la sociedad [15].

Aunque no resulta realista planear las acciones en el ciberespacio como las únicas importantes de las operaciones militares, si ha quedado manifiesta su gran capacidad ofensiva y, en consecuencia, resulta inexcusable prepararse para la obtención del nivel de Capacidad de Ciberdefensa Militar, CDM, suficiente para la defensa de los sistemas de mando y control propios que garanticen la libertad de acción en la conducción de las operaciones y proporcionen un

15. Véase PD1-001. Doctrina para el empleo de las Fuerzas Terrestres. ET-MADOC Mando de Adiestramiento y Doctrina. 2011. Granada.

adecuado nivel de seguridad [16] en el empleo de los sistemas de telecomunicaciones e información, CIS. Doctrinalmente las publicaciones del Ejército de tierra [17], incluyen inicialmente la capacidad de Ciberdefensa dentro de las actividades de la Función de Combate relativa a Protección. Sin embargo y dado el imparable desarrollo del ciberespacio como dominio de actuación, será necesario estudiar y actualizar próximamente su encuadre dentro del cuerpo doctrinal para adecuarse a las tendencias en este sentido.

Esta capacidad se debe conseguir a través de tres elementos fundamentales que contribuyan globalmente a la consecución completa de ella como son:

—defensa, que incluya las medidas y acciones de protección, prevención, detección, reacción, recuperación frente a los ataques, intrusiones, interrupciones u otras acciones no autorizadas que puedan comprometer la información y los sistemas que la manejan,
—explotación, que permita la recopilación, análisis y aprovechamiento de información de los ciberataques para determinar la procedencia e impacto, y
—respuesta, que incluya las medidas y acciones a tomar ante amenazas o ataques.

Aunque tradicionalmente los CIS tácticos se desenvolvían en entornos cerrados, actualmente las exigencias en operaciones requieren de mayores interconexiones con otros sistemas de agencias de cooperación, fuerzas de la nación anfitriona, organizaciones internacionales, e incluso ONG. Este podría ser el caso de futuras redes de misión, como la citada AMN. Una federación de redes entre la red clasificada de ISAF y las extensiones nacionales de las redes de los países de la Coalición. La mayoría de nuestros aliados, pondrán su capacidad militar de Mando y

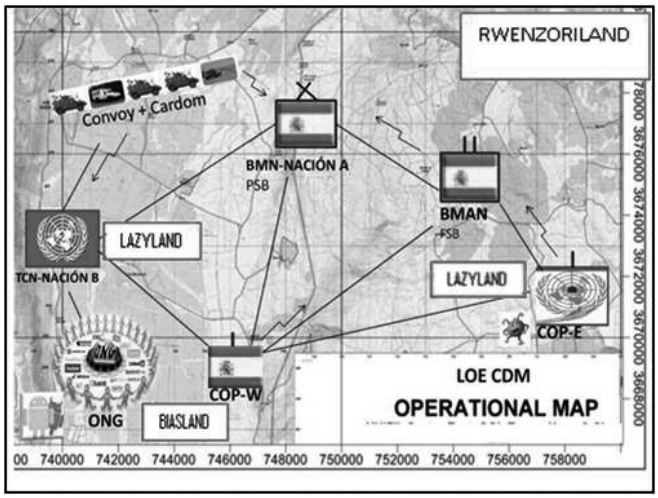
16. Precisamente uno de los argumentos principales en los que justifica EEUU su política de Ciberespionaje a raíz de la polémica por el caso Snowden.

17. Publicaciones Doctrinales de Segundo Nivel: PD2-001. Operaciones (aprobada en 2013) y PD2-002. Funciones de Combate. MADOC. Granada (pendiente de revisión final en mayo de 2013).

Control en Network Enabled Capability, —NEC, donde todo converge al protocolo de Internet, IP— con políticas adecuadas de ciberseguridad, pero habrá organizaciones que pueden no estar en sintonía, bien por utilizar distintas opciones tecnológicas o por aplicar diferentes niveles de seguridad, lo cual, requerirá de una capacidad de Ciberdefensa que permita trabajar con ellas.

A la vista por tanto de la relevante importancia de los beneficios del correcto uso del Ciberespacio para la Fuerza Terrestre, el Programa de Investigación referido puso en marcha un innovador ejercicio experimental de objetivo limitado LOE [18] con el inestimable apoyo del Instituto Tecnológico de la Marañosa (ITM). El LOE sirvió de novedosa y excelente plataforma de puesta en práctica de todos los trabajos conceptuales sobre Ciberdefensa llevados a cabo hasta ese momento por el Ejército de Tierra. A todo ello contribuían una serie de objetivos secundarios, principalmente consistentes en realizar simulaciones de ataques sobre los sistemas de información de Mando y Control de una agrupación táctica multinacional liderada por España que desplegaba ante una situación extrema de crisis en un escenario ficticio, Rwenzoriland.

Figura 8. Escenario táctico simulado del ejercicio de ciberdefensa. La operación multinacional de respuesta ante una crisis, se vio fuertemente condicionado por las actividades «ciberelectromagnéticas»



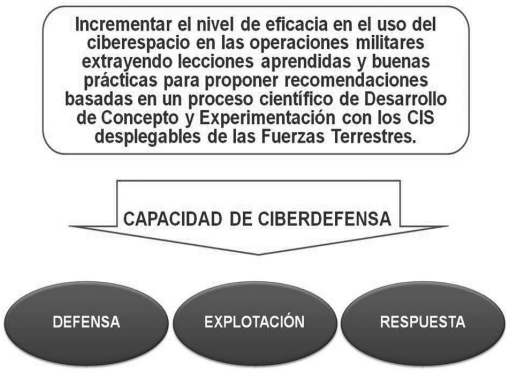
18. *Limited Objective Experiment*: LOE.

Una operación de apoyo a la paz, en la que estaban presentes distintos actores civiles y militares que interoperaban en el ciberespacio compartiendo información pero al mismo tiempo también vulnerabilidades que en algunos casos se traducían en catastróficas consecuencias. Los equipos de respuesta tácticos debieron concentrarse en analizar los patrones de ataque enemigos, esforzarse en mitigar sus propias vulnerabilidades, teniendo en cuenta parámetros como la superficie efectiva de ataque, tipo y número de puertos abiertos, capacidad de detección, de recuperación, etc., frente ataques de denegación de servicio DDoS, amenazas persistentes avanzadas, APT, etc.

Dirigido por su Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM), participaron distintas unidades de la Fuerza Terrestre FUTER como la Brigada de Transmisiones BRITRANS, el Mando de Operaciones Especiales MOE, el Cuartel General de Alta Disponibilidad CGTAD, el Mando de Apoyo Logístico MALE, distintos organismos del Ministerio de Defensa como el Centro de Operaciones y Seguridad de la WAN PG COS-DEF, etc. Fue fundamental la participación del centro de respuesta CERT de la Jefatura de Telecomunicaciones, Sistemas de Información, y Asistencia Técnica JCISAT.

En definitiva, un total de aproximadamente doscientos participantes provenientes del Órgano Central de la Defensa, del EMAD, del CIFAS, del Ejército de Tierra, la Armada y el Ejército del Aire, del Grupo de Delitos Telemáticos y Policía Judicial de la Guardia Civil, cuatro universidades destacando el papel activo de la de Granada desde su Centro de Servicios de Redes de Comunicaciones, CSIRC, como parte integrante junto con empresas punteras como Isdefe, S21sec, Innotec, Cidites, Repsol…, de la plataforma de ataque, así como de think-tanks como Syntagma, el USA *Cyber Security Forum Initiative*, y periodistas de distintos medios nacionales e internacionales que se hicieron eco del innovador evento.

Figura 9. Objetivo del primer ejercicio (LOE) de ciberdefensa experimental dirigido por el MADOC y ejecutado en el ITM en diciembre de 2012



El «escenario cibernético» incluía una operación de mantenimiento de la paz de la ONU en la que la OTAN estaba encargada de detener la violencia y las muertes de civiles debido a la inestabilidad en un estado fallido. La coalición multinacional que desplegaba en este escenario fue víctima de numerosos ciberataques con *defacements*, ataques DDoS, inyección SQL, *man in the middle*, captura de tráfico VoIP, perturbación de señales GPS, actividades de gestión de la percepción en las redes sociales, etc. Uno de los instrumentos destacado utilizado en el nivel táctico en el experimento, fue el centro de gestión ante incidentes de seguridad y administración de eventos (SIEM) basado en *Open Source Software Architecture*.

Todos los participantes y observadores mostraron su gran satisfacción por esta innovadora iniciativa del Ejército de Tierra a través de su Dirección de Investigación y Doctrina (DIDOM), aplicada por primera vez con un completo enfoque integral, —gracias a la estrecha colaboración con el ITM, la universidad y distintas empresas del sector de la ciberseguridad—, de las operaciones a un escenario táctico simulado pero muy próximo a la realidad. En palabras de uno de los participantes [19];

19. Véase «España y la Ciberdefensa». Artículo publicado en el Blog *La Ley en la Red* en ABC digital de Pablo García Mexiá. 08 de enero de 2013. Madrid. http://www.abc.es/blogs/ley-red/public/post/espana-y-la-ciberdefensa-14871.asp

Ejercicios como el aquí comentado pretenden justamente evitar que nuestro país pudiera algún día ser víctima de ataques de ese tipo. O, siquiera sea, limitar sus consecuencias. Nadie está jamás seguro del todo, y en menor medida aún cuando Internet y el mundo digital están de por medio. Pese a ello, y no es poco, España es bien consciente de la necesidad de «ciberdefenderse». Lejos de «cruzarse de brazos» ante estas graves amenazas, las Fuerzas Armadas españolas se preparan activamente en su contra. Las valiosas conclusiones obtenidas, fruto de una intensa colaboración con el sector digital y la comunidad científica, no deben dar pie a triunfalismo alguno. No obstante, sí que permiten demostrar que nuestras Fuerzas Armadas muy probablemente se encuentran entre las punteras en esta materia a escala mundial. Aliciente no pequeño para perseverar en esta línea.

> If the discussion is focused at the operational level of war, we find that cyberspace operations are actually quite similar to those in other domains [20]

Conclusiones y reflexiones finales

La ciberdefensa debe ser una capacidad militar más que implica y afecta desde el nivel estratégico al táctico a todas las armas y especialidades. No debe a pesar de su juventud considerarse más importante que otras necesarias en los dominios clásicos; tierra, mar, aire o espacio, pero debe enfocarse desde la perspectiva de que el ciberespacio se presenta de forma permanente y transversal a los anteriores en todas las operaciones y actividades de las mismas.

Deberá ejecutarse en un complejo espectro de operaciones en el que será imprescindible contar con un enfoque integral ante el dinámico y complejo entorno operativo. Los Ejércitos y la Armada son responsables de sus sistemas de información para mando y control, C2IS, mientras que el Mando Conjunto de Ci-

20. Major General Brett T. Williams, HQ USAF. Jefe de Operaciones 2011. Anteriormente fué Director de Command, Control, Communications, and Computer C4IS, Systems, U.S. Pacific Command.

berdefensa, MCCD, fijará su interés en la defensa nacional. Las ciber-operaciones podrán ser defensivas u/y ofensivas englobando las tres subcapacidades expuestas de Defensa, Explotación y Respuesta. Cuando se decida desde el nivel correspondiente llevar a cabo una respuesta, ésta deberá ser multidisciplinar pues será la única válida para conseguir la sinergia de esfuerzos de una nación y no se entiende la actuación aislada de actores en este dominio global y común de interés para todos ellos. En territorio nacional será coordinada por el General Jefe del Mando Conjunto de Ciberdefensa, MCCD, y en zona de operaciones podrá ser necesario frecuentemente que lo sea por el Comandante de la Fuerza táctica desplegada, COMFORCE.

Si se decide hablar de ciberguerra, entonces debe ser considerada como una componente más de un conflicto armado generalizado y su posibilidad de empleo como un hecho probable [21], teniendo en cuenta que las potenciales amenazas en el uso del ciberespacio, se multiplican en zona de operaciones y en ese nivel tendrán que enfrentarse las fuerzas terrestres con mayor protagonismo y esfuerzo. En cualquier caso,

> …después de un tiempo de experiencias y lecciones identificadas por muchos estados en el ciberespacio, la definición de ciberguerra continúa presentándose compleja. Ciertas actividades, como son las distintas formas de terrorismo, se centran en convocar el miedo de la población para conseguir objetivos sociales o políticos normalmente, y no por ello se puede hablar formalmente de guerra, al menos como la entendemos tradicionalmente, sería muy desacertado.
>
> Al mismo tiempo, se ha asociado con actos de ciberguerra a determinadas acciones que han infligido daños generalizados en cualquiera de las dimensiones sociales, económicas, o políticas de ciertas naciones y que han excedido a lo que se podría denominar como un simple perjuicio. Puede ser comprensible el hecho de que el término ciberguerra es fácil de recordar y por ello suele emplearse alegremente al observar cualquier experiencia negativa que se produzca en el ciberespacio, sin analizar en profundidad el alcance

21. Conclusiones del Director de Investigación, Doctrina, Orgánica y Materiales (DIRDOM), General de División D. Alfredo Ramírez Fernández, en la presentación de los productos finales del programa de investigación sobre Ciberdefensa. 07 de marzo de 2013. Granada.

del mismo. Ciberguerra o no, lo que están muy claros son los amplios puntos en común con otros conceptos como el de ciberterrorismo, empezando por el dominio global común de actuación, el ciberespacio, y siguiendo con las tácticas, técnicas y procedimientos empleados. Estas analogías nos hacen comprender la necesidad urgente de actuar enérgicamente desde una aproximación holística de todos los actores que deben implicarse en la defensa del bienestar, intereses y valores de los estados libres y democráticos.

Desde el mero plano personal hasta el colectivo, la sensatez y el sentido común deberían presidir unas actuaciones acordes con cada nivel de responsabilidad. De esta forma, sería posible mantenerse lejos de la histeria que pueda conducir al bloqueo del normal uso de las tecnologías y del riesgo al mismo tiempo de que se motive la evitación de su empleo por desconocimiento de las mismas, además de caer en el peligro de la excesiva despreocupación por las amenazas y vulnerabilidades de esa utilización —la ciberindiferencia—. En consecuencia, se trata de alcanzar un índice de preocupación, —ciberinquietud— proporcional y ajustado a cada nivel, que permita continuar disfrutando sin miedo de los grandes avances tecnológicos alcanzados y en imparable progresión.

Por tanto, la protección del ciberespacio debe ser una prioridad dentro de las líneas de actuación estratégicas de la seguridad y llegado el caso, las Fuerzas Armadas como actores clave deben estar preparadas no sólo para su defensa, también para ejecutar acciones ofensivas si así se ordenase porque lo motivase la situación o la misión. Llegado ese momento, no cabría duda de que efectivamente se estaría combatiendo en una ciberguerra [22].

La amplia gama de amenazas a afrontar, así como la dificultad para su identificación, requerirán de una cooperación, concienciación y preparación al más alto nivel y con un enfoque holístico en un dominio global común donde convergen las acciones «ciber» con las del Espectro Electromagnético, EEM. Para ello se deberá seguir impulsando la organización y preparación e interoperabilidad de los centros de respuesta. Estos centros CERT

22. Para profundizar sobre reflexiones sobre esta dicotomía entre la excesiva preocupación o la indiferencia por las actividades en el ciberespacio, ver artículo: ¿Es la ciberguerra un auténtico desafío a la seguridad y la defensa» Revista internacional Fuerzas de defensa y seguridad. Núm 408 de abril de 2012. Madrid.

(*Computer Emergency Response Team*), CSIRT (*Computer Security Incidente Response Team*), etc., convenientemente dotados en material y personal, deben estar preparados y especializados en ofrecer la solución más adecuada para dar una respuesta común, eficaz y eficiente a estos nuevos riesgos. Será fundamental su plena integración desde el nivel estratégico al táctico teniendo siempre presente la compleja dificultad de obtener una alerta temprana eficaz acerca de actividades en el ciberespacio en contra de los intereses de seguridad nacionales. La atribución de los orígenes de las mismas, en tal caso, continuará siendo un problema que mantendrá el recelo y la desconfianza entre actores en conflicto sufriendo con frecuencia en tiempo de paz actividades muy próximas al espionaje y llevadas a cabo por «ciberejércitos secretos» no reconocidos.

Las tecnologías de la información y comunicaciones, TIC, continuarán su imparable progresión y seguirán constituyendo los vehículos de las actividades en el ciberespacio. Es vital que España continúe con las acciones de I+D+i orientadas hacia una Ciberseguridad completa en la que el sector empresarial tenga un papel relevante por la seguridad nacional,y por tanto resulta vital un enfoque integral de la ciberdefensa.

Ahora, una vez que el MADOC ha iniciado las actividades de investigación y experimentación de las operaciones de las Fuerzas Terrestres en este llamado a menudo quinto dominio, extrayendo lecciones aprendidas y recomendaciones a nivel nacional, se presenta la oportunidad de extender dicha investigación aportando su experiencia táctica en el ámbito multinacional combinado. Uno de los campos de actuación que se muestra se encuentra en el marco de los experimentos multinacionales MNE, donde el MADOC viene colaborando desde el año 2008. En concreto, la «Campaña Multinacional de Desarrollo de Capacidades» «Multinational Capability Development Campaign» —MCDC en desarrollo entre 2013 y 2014—, se orienta en esta ocasión al análisis de la problemática de proyectar una fuerza combinada en un Área de Operaciones con la libertad de acción suficiente para cumplir su misión, es decir, garantizando el denominado Acceso Operacional, donde el Ciberespacio es uno de los principales dominios en disputa.

Las Fuerzas Armadas a través de las acciones ya iniciadas y con su proa puesta en alcanzar la capacidad operativa plena del Mando Conjunto de Ciberdefensa, continuarán dando su servicio a España en todo aquello que afecte a sus intereses nacionales, también en el Ciberespacio. Este objetivo crucial y prioritario continuará siendo complementado con todas las iniciativas en marcha como la participación en la referida campaña MCDC a través del MADOC con el apoyo empresarial y académico, en la que está planeado que en 2014 se reproduzca el experimento LOE aprovechando muchos de sus innovadores elementos implementados en el ITM; el escenario simulado, la metodología, etc., pero en esa ocasión en ambiente multinacional. Todo ello, motivado fundamentalmente por el interés expresado en el contexto internacional por parte de otros países sobre la experiencia y el importante camino recorrido por nuestra nación. Para España por tanto, constituye una satisfacción y todo un reto, pero al mismo tiempo, ¡toda una oportunidad!

MISIONES Y RETOS FOCALIZADOS EN EL CIBERESPACIO

Javier Bermejo Higuera [*]

Resumen

Es indudable la importancia de la potenciación de la I+D+i como medio de estar a la vanguardia en las tecnologías de seguridad de la información y comunicaciones y abordar los diferentes retos que supone el ciberespacio. En este contexto el Instituto Tecnológico «La Marañosa» ha creado una Unidad de Ciberseguridad, con la misión de control, seguimiento, investigación y desarrollo de las tecnologías que permitan mejorar la seguridad de los sistemas de información y comunicaciones de las Fuerzas Armadas. En la ponencia monografía se presenta un resumen de los principales retos o misiones relacionados con el ciberespacio, en los que inicialmente está trabajando dicha unidad: infraestructuras de experimentación en ciberdefensa, desarrollo de software seguro, protocolos seguros e investigación y análisis de malware.

Introducción

Actualmente los sistemas de información y comunicaciones (CIS) de las Fuerzas Armadas (FAS) están inmersos en un proceso de adaptación al concepto Network Enable Capability (NEC) con el objetivo de incrementar sus capacidades de mando y control.

[*] Javier Bermejo Higuera es Comandante de Ingenieros Politécnicos del Ejército de Tierra, Jefe de la Unidad de Seguridad del Área TICS del Instituto Tecnológico «La Marañosa» (ITM) del Ministerio de Defensa.

Las nuevas plataformas aéreas ya disponen de sistemas de comunicaciones para recibir y transmitir información constantemente; los sistemas de defensa aérea son teleoperados por ordenador; los sistemas de inteligencia, vigilancia y reconocimiento (ISR) recogen tanta información que el desafío está en obtener los datos críticos; las unidades de infantería disponen de sistemas de comunicación de banda ancha, sistemas de posicionamiento (FFT) y dispositivos de visión nocturna, en todos ellos existen dispositivos de proceso que representan una fortaleza pues incrementan la capacidad de combate, pero que también podrían convertirse en una debilidad pues presentan vulnerabilidades, lo que exige la adopción de medidas para su protección, con la consecuente y necesaria puesta en marcha de capacidades de ciberdefensa.

En el documento Visión del JEMAD [1] se indica: «En la actualidad la mayoría los sistemas de mando y control, e información militar, así como determinados sistemas de combate y de control de plataformas y armas, están conectados a través de redes militares de comunicaciones que en mayor o menor medida también están expuestos a las diferentes amenazas que existen en el ciberespacio, disponen de interconexiones a otros sistemas, ya sean OTAN, UE o de países aliados; forman parte de una federación de redes en el ámbito operativo; o sus enlaces se realizan en ciertas ocasiones a través de infraestructuras civiles, lo que complica el mantenimiento de la seguridad».

La guerra cibernética ha supuesto una sorpresa para gobiernos y ejércitos de todo el mundo, como se puso de manifiesto en Estonia en el año 2007, cuando un ataque cibernético dejó desconectado el país durante una semana, dejando patente la carencia de organización y medios de la OTAN para hacer frente a este tipo de amenazas. Un año más tarde, cuando Rusia invadió Georgia, el ataque convencional fue precedido por un asalto en el ciberespacio (supuso uso de una nueva dimensión del combate la quinta); cayendo gran número de ordenadores estatales en poder de hackers rusos y obligando al Ministerio de Asuntos Exteriores a

1. Véase *Visión del JEMAD de la Ciberdefensa Militar*. Estado Mayor de la Defensa (2011).

trasladar su web. La obtención de capacidades cibernéticas se ha convertido en un aspecto crítico de la guerra actual y, como tal, debe integrarse en la doctrina militar. El ciberespacio ha pasado a ser el quinto dominio de la guerra, uniéndose a los tradicionales tierra, mar, aire y espacio. Un arma clave en este dominio es el malware, nuevo instrumento de proyección de poder e influencia.

Por otra parte en el entorno civil, los ataques cibernéticos son cada vez más frecuentes, más organizados y más costosos en el daño que infligen a las administraciones públicas, empresas, economías, redes de transporte, redes de suministro y otras infraestructuras críticas (desde la energía a las finanzas), pudiendo incluso llegar a ser una amenaza a la prosperidad, la seguridad y la estabilidad de un país. Unidades militares y servicios de inteligencia extranjeros, grupos de crimen organizado, grupos terroristas o extremistas pueden ser el origen de tales ataques.

El Departamento de Defensa estadounidense aprobó, en julio de 2011, una «Estrategia de Operaciones en el Ciberespacio» en la que destaca la potenciación de la I+D+i como medio de estar a la vanguardia en estas tecnologías y abordar los diferentes retos que supone el ciberespacio. Queda pues suficientemente justificado y de vital importancia el fomentar las actividades de I+D+i como forma de mejorar la seguridad los sistemas CIS de las FAS.

En este contexto el Área TICS del Instituto Tecnológico «La Marañosa» (ITM) ha creado una Unidad de Seguridad, con la misión de control, seguimiento, investigación y desarrollo de las tecnologías que permitan cubrir las carencias de seguridad detectadas en los sistemas de comunicaciones y sistemas de información de las FAS. Los principales retos o misiones relacionados con el ciberespacio en los que inicialmente está trabajando dicha unidad son los siguientes:

—Infraestructuras de experimentación en Ciberdefensa.
—Desarrollo de software seguro.
—Protocolos seguros.
—Investigación y análisis de malware.

Infraestructuras de experimentación en ciberdefensa

Introducción

Tradicionalmente la seguridad de estos sistemas se ha enfocado exclusivamente desde la perspectiva de «Ciberseguridad», centrada en la defensa y protección de sus redes y frente a intrusiones en las mismas; recientemente, ha surgido una nueva disciplina, la «Ciberdefensa», subconjunto de la anterior, que tiene lugar en la fase operativa y se materializa mediante los ciberataques y su defensa.

La OTAN define Ciberdefensa [2] como «la capacidad de asegurar y salvaguardar el suministro de los servicios CIS en operaciones, en respuesta a posibles inminentes acciones maliciosas originadas en el ciberespacio». Entre las capacidades que abarca podemos incluir las siguientes:

—Detección de ataques cibernéticos y actividades maliciosas.
—Prevención y mitigación de ciberataques.
—Recuperación frente a ciberataques.
—Evaluación dinámica del riesgo.
—Conciencia de la situación, en cuanto a la capacidad de evaluar el estado de la seguridad de los sistemas y los daños producidos por los ciberataques.
—Toma de decisiones en tiempo oportuno.
—Defensa activa (hacking ético).
—Colaboración y compartición de información de Ciberdefensa.
—Análisis de malware.

Hasta la fecha, las nuevas tecnologías de seguridad, relacionadas con Ciberdefensa, se han probado y validado solamente en instalaciones de investigación privadas de escala media o reducida, que pueden resultar no ser representativas de redes operativas grandes, como pueden ser las redes internas del Ministerio de Defensa como pueden ser las redes de Propósito General y Man-

2. Véase Hallingstad, Geir y Dandurand, Luc, *Cis Security (Including Cyber Defence) Capability Breakdown*, 2011.

do y Control o la porción del Internet que podría implicarse en un ataque, careciendo por tanto del necesario rigor científico las conclusiones o enseñanzas que pudieran inferirse de los experimentos que se pudieran realizar.

En base al conocimiento que se tiene actualmente, a nivel del Ministerio de Defensa, existe también una carencia de infraestructuras de experimentación que proporcionen un entorno controlado para la realización de pruebas o ensayos, que incluya redes de soporte de comunicaciones, plataformas virtualizadas, herramientas, metodologías y procesos que permitan la experimentación, investigación y el desarrollo avanzado de las nuevas tecnologías de seguridad.

Básicamente se aspira a implantar, operar y mantener un Centro de Experimentación en tecnologías de ciberdefensa, abierto a una comunidad amplia de usuarios tanto del propio Ministerio de Defensa, como con el entorno académico y universitario u otras instituciones dedicadas a la investigación, o el entorno empresarial. Se pretende que el centro permita el intercambio y la colaboración entre investigadores en las tecnologías de la seguridad, en el cual los investigadores del ITM, la Universidad y desarrolladores de la industria, puedan experimentar con tecnologías de seguridad potenciales en condiciones realistas. Todo ello supondrá además una oportunidad para coordinar los esfuerzos de investigación y desarrollo y lograr sinergias entre el entorno civil y militar.

Las principales metas que se pretenden alcanzar con la implantación de esta infraestructura de investigación, serían:

—Facilitar la experimentación científica y la identificación de las nuevas amenazas cibernéticas, incluso a medio plazo.
—Desarrollo y experimentación de conceptos (CD&E) y de estrategias militares en todo lo relativo al ámbito de la Ciberdefensa y en el de su integración con otras capacidades militares.
—Proporcionar una plataforma segura de experimentación, aislada de los entonos de producción, redes de comunicaciones propietarias e internet.
—Proporcionar el acceso controlado a un amplio espectro de usuarios, tanto del Ministerio de Defensa, del ámbito académico, o del empresarial.

—Desarrollo científico de metodologías de prueba rigurosa que sean eficaces para la defensa contra ataques a la infraestructura en red y los sistemas de información.
—Desarrollo de experimentos para obtener una comprensión más profunda de los diferentes tipos de ataques cibernéticos, de las nuevas técnicas y tecnologías de defensa a través de la evaluación de escenarios de pruebas diferentes, así como el grado de afección en Internet, redes propietarias, sistemas de información y a los usuarios.
—Difusión del conocimiento para contribuir al desarrollo de las capacidades de Ciberdefensa.
—Desarrollo de prototipos (nuevos desarrollos), estableciendo líneas de referencia para la validación, como podrían ser: topología de ataque, dispositivos de defensa, métricas de medida, etc.

Requerimientos de esta infraestructura de experimentación

Las líneas de investigación y tecnologías a desarrollar y probar en esta infraestructura de experimentación, serían de dos tipos: unas de naturaleza dual aplicables a los entornos civil y militar y otras aplicables sólo al entorno militar. En conjunto, abarcarían una amplia gama de tipos generales de ataques y herramientas de defensa o combinaciones de ellos. En concreto las tecnologías y líneas de investigación a experimentar, pueden ser las siguientes:

—*Tecnologías duales aplicables al entorno militar y civil:* gestión y monitorización de eventos de seguridad, correlación de eventos, detección de intrusos y políticas de control de acceso a datos y redes, simuladores, sistemas anti-fuga de datos, neutralización de «botnets», propagación de gusanos, gestión dinámica del riesgo, mitigación de ataques de denegación de servicio distribuido (DDoS) y estudio de ataques contra la infraestructura de enrutamiento de redes de comunicaciones, inteligencia (recolección de información de fuentes abiertas, filtrado de datos y alerta temprana) y seguridad de arquitecturas orientadas a servicios.
—*Tecnologías aplicables sólo al entorno militar:* mecanismos de federación seguros en entornos militares, tecnologías de

cifra nacional, sistemas de alta disponibilidad (robustos), compartición de información de forma segura, sistemas y redes de seguridad multinivel, investigación y desarrollo de malware, automatización de malware, análisis de vulnerabilidades en software y malware y creación de «exploits».

Consecuentemente, una infraestructura de experimentación válida para poder abordar las tecnologías anteriores deberá incluir: diferentes escenarios de ataque, simuladores, generadores de topología capaces de simular enlaces de comunicaciones con diferentes anchos de banda, retardo, jitter, etc., generadores de tráfico de fondo que simulen el tráfico normal en una red, conjuntos de datos de malware y herramientas para su análisis, recolección de «log,s» y herramientas para monitorizar y poder analizar los resultados de las pruebas.

Asimismo se requiere el desarrollo de metodologías de prueba rigurosas en entornos controlados de la infraestructura experimental para obtener una evaluación realista, repetible y coherente de los mecanismos para mitigar los supuestos ataques a gran escala.

Un problema importante, a resolver en cada experimento, será el cuantificar el alcance de los modelos para poder simular el entorno real (red operacional o porción de internet) y la selección o creación de métricas adecuadas para poder evaluar los diversos mecanismos equipos o sistemas de defensa.

Los requisitos que deben servir pues de guía para la implantación de este tipo de infraestructuras se pueden resumir en los siguientes:

—Entorno *variable y versátil* con capacidad para soportar múltiples escenarios de prueba y experimentación.
—*Seguridad y aislamiento*: la infraestructura de experimentación debe estar completamente aislada para evitar la propagación de software dañino al entorno de producción, redes operacionales o incluso internet.
—La infraestructura debe ser capaz de soportar la ejecución y monitorización de *diferentes experimentos a la vez*.
—Debe ser capaz de *simular fielmente entornos reales de producción*, como pueden ser redes operacionales o porciones de internet.

—*Economía de medios*, para poder afrontar de forma práctica y económica el requisito anterior se requerirá una plataforma virtualizada, con capacidad de ejecutar al menos 1.000 máquinas virtuales de forma simultánea y poder de almacenamiento de 10.000.
—Deberá disponer de *varios entornos de virtualización* (simulación, experimentación, análisis de malware, cuarentena, etc.), alojados en el mismo equipamiento físico e incluso entornos mixtos, con mezcla de equipos virtuales y físicos para poder realizar pruebas de evaluación de estos últimos.
—*Accesibilidad*, para permitir al acceso y su control físico y por red a usuarios externos de otros organismos a través de redes privadas virtuales (VPN).
—*Escalabilidad*, capacidad de realizar conexiones seguras mediante VPN con otras infraestructuras de experimentación de la Administración o el entorno empresarial, como forma de aumentar el alcance de los experimentos a realizar.
—*Flexibilidad* para la creación y gestión de los experimentos.
—Repetitividad, el entorno debe permitir repetir los experimentos realizados, con control de las diferentes variables del entorno.
—*Funcionalidad*, el entorno deber debe disponer de gran cantidad de herramientas.
—*Disponibilidad:* debería disponer de arquitecturas de conmutación y firewall en alta disponibilidad redundados.
—*Obtención del malware*, para poder obtener conjuntos de datos del malware para la realización de experimentos y análisis se dispondrá de una Honeynet en una DMZ y otra en Internet.
—Dispondrá de un entorno aislado para *análisis y reingeniería de malware* con equipamiento software necesario para la realización de análisis estático y dinámico, disponiendo de un acceso seguro a la Honeynet para recolección malware.
—Deberá disponer de *simuladores de técnicas de ataque y defensa* de Ciberdefensa, con el objeto de poder formar y entrenar a las diferentes unidades del Ministerio de Defensa con responsabilidades en seguridad.
—El entorno debe disponer de *mecanismos de defensa* ante ejecuciones descontroladas de software dañino.

En resumen, la infraestructura de experimentación para Ciberdefensa deberá contar con un banco de pruebas con capacidad de poder trabajar con aproximadamente 1.000 equipos virtuales y varios físicos, cada uno con múltiples tarjetas de interfaz de red y gran cantidad de memoria, y un importante número de routers de diferentes casas comerciales. Dentro de este entorno, la red debe proporcionar la complejidad topológica suficiente para emular una representación reducida pero funcional precisa de la estructura jerárquica de las redes operacionales del Ministerio de Defensa o una porción de internet real, y para aproximarse a la mezcla de tráfico benignos y maligno producidos durante los ataques.

Arquitectura de la infraestructura de experimentación

En base a los requisitos presentados en el apartado anterior, en el presente punto se presenta la descripción resumida de una arquitectura de la Infraestructura de Experimentación tanto a nivel físico en cuanto equipamiento que debería contener, como a nivel lógico en cuanto a sus subsistemas componentes, capacidades y servicios así como las funcionalidades y flujos que se requieren para un entorno experimental seguro.

La infraestructura se implantaría utilizando una plataforma virtualizada, que integraría equipamiento físico de diversos fabricantes, de forma que en un entorno de experimentación concreto sea posible incluir tanto equipos físicos como virtualizados.

A nivel físico, la infraestructura constaría básicamente de un conmutador de núcleo de gran capacidad de conmutación y ancho de banda en arquitectura de alta disponibilidad que además implementaría las diferentes redes de área local virtual (VLAN) de los diferentes subsistemas de la infraestructura de experimentación. A nivel lógico es el firewall el que tendrá toda la responsabilidad de enrutamiento y comunicación entre los diferentes segmentos de red VLAN, algunos de los cuales deben permanecer aislados. Cada segmento tendría, que permanecer aislado, además de conexión con el firewall, que hará de puerta de enlace por defecto.

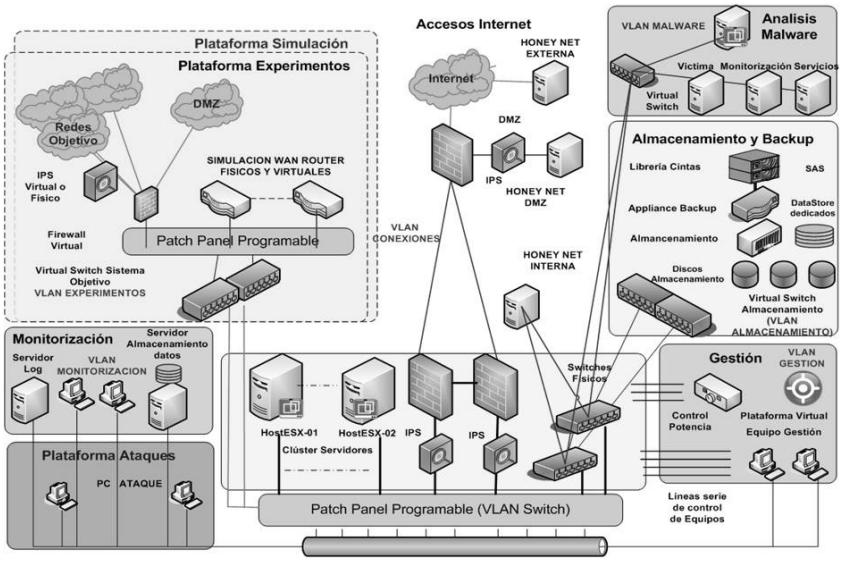
La infraestructura contaría además con una DMZ de dos capas implementada en base a dos firewall de diferentes fabricantes, albergando en una de sus zonas una honeynet. El firewall externo

también se utilizaría además servidor de túneles de la VPN con el propósito de enrutar el tráfico de acceso de investigadores del exterior o conexión con otras infraestructuras de experimentación.

La arquitectura se compondría de los siguientes subsistemas, que podrán ser implementados con equipamiento virtual, físico o combinación de ambos, en la figura 1 se representa un diagrama lógico de la misma:

—Subsistemas de Gestión y Control.
—Subsistemas de Análisis y Monitorización de Datos.
—Subsistema de Experimentos.

Figura 1. Diagrama lógico Infraestructura Experimentación



—Subsistema de Ataque.
—Subsistema de Almacenamiento.
—Subsistema Recolección de Malware. Subsistema Análisis de Malware.
—Subsistema de simulación.
—Subsistema Acceso Internet.

Desarrollo software seguro

Tradicionalmente en el MINISDEF se ha bastionado el software de base (sistemas operativos, bases de datos, etc.) sin tener en cuenta que los sistemas de información, mando y control, etc., desarrollados específicamente para la FAS, son inherentemente complejos y sus implementaciones y desarrollos contienen fallos y vulnerabilidades de seguridad que potencialmente pueden ser explotadas por hackers, organizaciones cibercriminales o unidades militares de otros países.

Además erróneamente, a pesar de los datos convincentes de lo contrario, se sigue confiando que la implantación de dispositivos de seguridad de red: cortafuegos, almacenamiento y análisis de logs, sistemas de detección de intrusos, sistemas de gestión de acceso y el cifrado del tráfico son medidas suficientes para proteger los sistemas. Los atacantes buscan el descubrimiento de fallos en el software relacionados con la seguridad del sistema, convirtiéndose así en una vulnerabilidad con un impacto y riesgo asociado para las FAS.

Se puede definir la seguridad del software como:

> El conjunto de técnicas y buenas prácticas utilizadas para la obtención de un software robusto frente ataques maliciosos, libre de vulnerabilidades, ya sean intencionalmente diseñadas o accidentalmente insertadas durante ciclo de vida, de forma que se asegure su integridad, disponibilidad y confidencialidad.

Un aspecto importante de la seguridad del software es la confianza y la garantía de que funciona conforme a su especificación y diseño y que es lo *suficientemente robusto para soportar las amenazas que puedan comprometer el funcionamiento esperado en su entorno de operación.*

Se considera por tanto, en base a lo expuesto anteriormente, la necesidad de disponer por las FAS de software fiable y resistente a los ataques, de confianza, es decir que el número de vulnerabilidades explotables que posea sea el mínimo posible. Las principales propiedades que distinguen al software de confianza del que no los es:

—*Integridad:* capacidad que garantiza el código del software, activos manejados, configuraciones y comportamiento no pueda ser o no ha sido modificada o alterada por personas, entidades o procesos no autorizados.
—*Disponibilidad*: capacidad de garantizar que el software es operativo y accesible por personas, entidades o procesos autorizados de forma que se pueda acceder a la información y a los recursos o servicios que la manejan, conforme a las especificaciones de los mismos.
—*Confidencialidad:* capacidad de preservar que cualquiera de sus características, activos manejados está ocultos a usuarios no autorizados, de forma que se garantice que sólo las personas, entidades o procesos autorizados pueden acceder a la información.

Estas tres primeras serían las propiedades fundamentales mínimas que debería disponer todo software, a las que habría que añadir las siguientes:

—*Fiabilidad:* capacidad de funcionar de la forma esperada en todas las situaciones a la que estará expuesto en su entorno de funcionamiento, es decir que la posibilidad de que un agente malicioso pueda alterar la ejecución o resultado de una manera favorable para el atacante está significativamente reducida o eliminada.
—*Autenticación:* capacidad que permite a un software garantizar que una persona, entidad o proceso es quien dice ser o bien que garantiza la fuente de la que proceden los datos
—*Trazabilidad:* capacidad que garantiza la posibilidad de imputar las acciones relacionadas en un software a la persona, entidad o proceso que la ha originado.
—*Robustez:* capacidad de resistencia y tolerancia a los ataques realizados por los agentes maliciosos (malware, hackers, etc.).
—*Resiliencia:* capacidad de un sistema de software debe ser capaz de recuperarse ante cualquier tipo de exposición o daño causado por agentes maliciosos y reanudar su operación en o por encima de cierto nivel mínimo predefinido de servicio aceptable en un tiempo oportuno.

Las propiedades que distinguen al software de confianza se ilustran en la Figura 2.

Figura 2. Propiedades seguridad del software

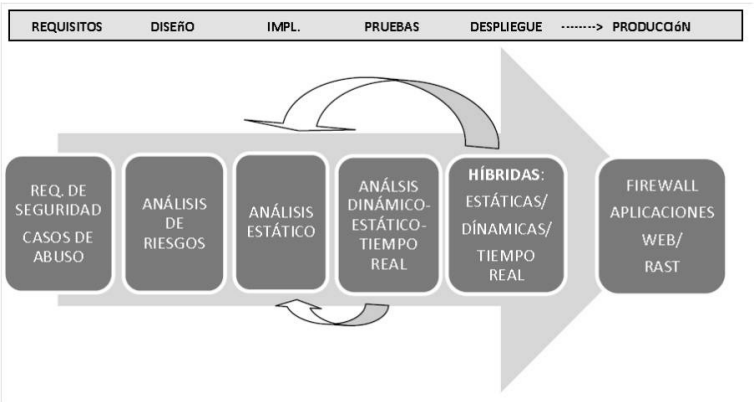
La Unidad de Seguridad del ITM ha establecido, en este campo, un servicio basado en la adopción de una metodología que tiene por objetivo mejorar la seguridad y calidad del software desde las *fases de análisis, diseño, desarrollo, despliegue, pruebas y operación* del ciclo de vida de desarrollo una aplicación o sistema de información, acometiendo el diseño, implementación y chequeo de la seguridad desde el principio de su desarrollo.

La metodología tomada como base [3] consiste básicamente en un nuevo modelo del ciclo de vida de desarrollo de software, con la que se pretende obtener un software seguro desde el comienzo de la fase de desarrollo utilizando de diversas técnicas y herramientas según la fase el ciclo de vida en la que nos encontremos, destacándose las siguientes:

3. Bermejo Higuera, Juan Ramón, *Estudio de técnicas automáticas de análisis de vulnerabilidades de seguridad en aplicaciones web*. Trabajo Fin de Máster UNED, 2011, pags. 47-48.

—*Requisitos de seguridad*: UML seguro, derivación de casos de abuso, análisis de riesgos.
—*Diseño*: análisis de riesgos
—*Codificación: análisis estático de código fuente / ejecutable.*
—*Pruebas:* análisis dinámico, estático, tiempo real.
—*Implantación*: híbridas de análisis estático-dinámico / hibridas de análisis estático-dinámico-tiempo real.
—*Producción:* análisis en tiempo real.

Figura 3. Modelo ciclo vida del software



El análisis estático de código fuente se considera la actividad más importante de entre las siete mejores prácticas que se han de realizar en el curso del desarrollo de una aplicación.

Protocolos seguros

Las principales actividades que se están llevando a cabo en el ámbito del Protocolos Seguros han sido sugeridas y guiadas por el Centro Criptológico Nacional (CCN), principalmente se centran en:

—Apoyo al CCN en la verificación y validación de algoritmos de cifrado software y su implementación hardware.
—Investigación sobre la aplicabilidad de los nuevos algoritmos de cifrado en las tecnologías de Defensa.

En este sentido se ha implementado un Laboratorio de Pruebas de Interoperabilidad de protocolos seguros, con las siguientes capacidades:

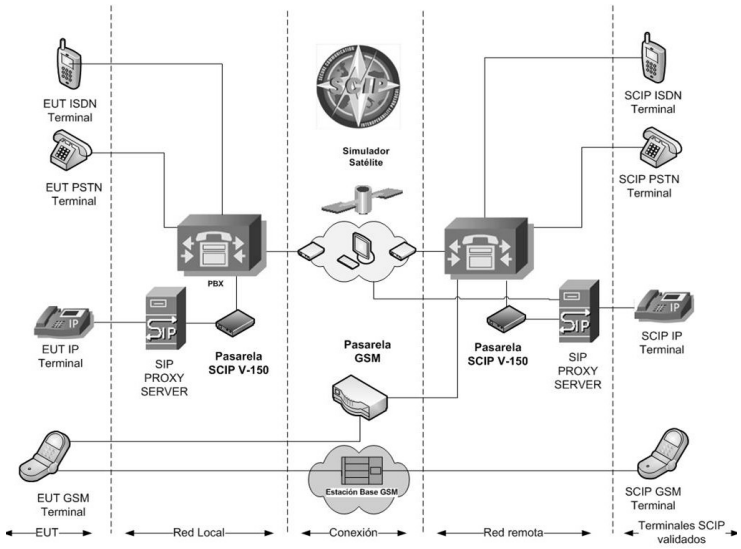
—*Banco de pruebas del Protocolo de interoperabilidad de Comunicaciones Seguras (SCIP),* para determinar las pruebas de conformidad, interoperabilidad y gestión de clave del protocolo, de forma se asegure que diferentes soluciones de los proveedores de terminales de voz segura, operen sobre redes heterogéneas, mediante el uso de estándares abiertos.

—Banco de pruebas de las diferentes implementaciones del protocolo IPSEC, en cuanto a conformidad con el estándar, rendimiento, interoperabilidad y sugerencias de configuración.

Adicionalmente se está realizando trabajos para la construcción de un futuro banco de pruebas de interoperabilidad para el protocolo Network and Information Infrastructure (NII) Internet Protocol (IP) Network Encryption (NINE), futuro protocolo de encriptado a nivel de red de la OTAN.

El objetivo del banco de pruebas de interoperabilidad SCIP, es la realización de los planes de pruebas estipulados a todos aquellos productos que utilicen protocolos de comunicaciones seguras SCIP, para la obtención de su certificación por parte del CCN. La topología del banco de pruebas realizado se muestra en la figura 4.

Figura 4 Banco de pruebas interoperabilidad SCIP



El equipamiento con el que cuenta en banco de pruebas es el siguiente:

—Centrales de voz IP privadas (PBX) basadas en software libre Asterisk.
—Pasarela de voz comercial V.150.1 SCIP.
—Teléfonos IP, analógicos y RDSI.
—Pasarela GSM.
—Proxy SIP Server.
—Simulador Satélite.
—General Dynamics SCIP Endpoint y Test Tool.
—SCIP endpoint nacional.

Investigación y análisis de malware

Un nuevo instrumento de proyección de poder e influencia y arma clave en el ciberespacio es el código malicioso, en adelante malware. Conocer la estructura, funcionamiento e interacción del malware, aportará una valiosa información, no sólo para el diseño y desarrollo de contramedidas eficaces, sino también para:

—Conocer el origen de un ataque e identificar al intruso.
—Evaluar la capacidad de detección de malware de los sistemas de protección del Ministerio de Defensa
—Evaluar los daños causados por la intrusión y acciones del malware.
—Descubrir otras máquinas que han sido afectadas por el mismo malware.
—Identificar la vulnerabilidad que fue aprovechada por el malware para poder diseñar acciones de respuesta necesarias y adecuadas.
—Determinar el nivel de sofisticación del malware.
—Aprendizaje para obtener la base de conocimiento futura que permita la creación de «exploits».

En este campo actualmente se está trabajando en dos áreas:

—*Desarrollo de una metodología*, técnicas y métodos de análisis y reingeniería de malware utilizando la experimentación y con el propósito de obtener un análisis completo del ciclo

de vida del malware; su comportamiento, métodos de ocultarse, ofuscación de código, sistemas de actualizaciones y comunicaciones. Los pasos que podrían comprender esta metodología serán, en un principio:

  —*Clasificación del Malware:* realización de una línea base del equipo víctima en base a la utilización de diferentes herramientas, obteniendo datos de inicio para poder realizar las siguientes fases.

  —*Análisis Dinámico*: ejecución y estudio de malware 'en vivo' en un entorno de laboratorio, la recogida y análisis de datos.

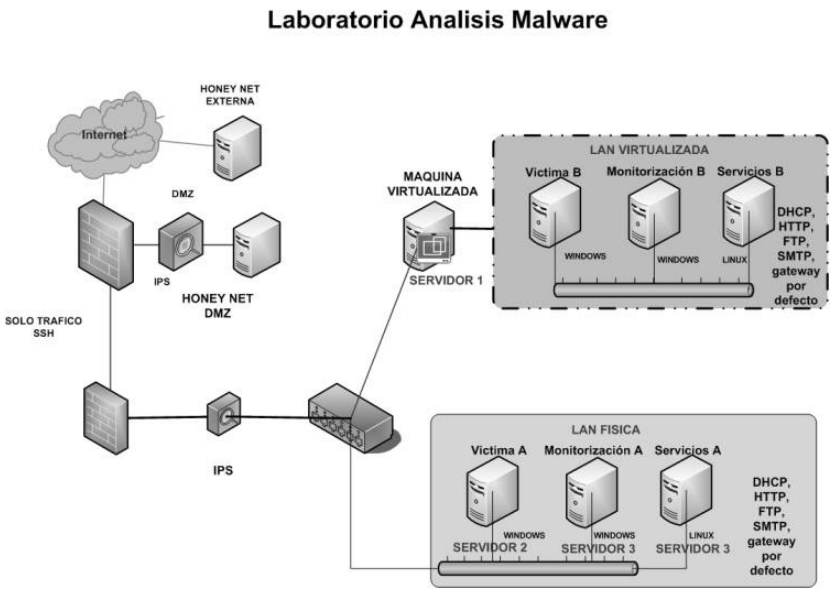
—Análisis estático y dinámico de su código.

—El grado de complejidad de las técnicas y el nivel conocimiento necesarios para analizar malware es proporcional al nivel de sofisticación del mismo, estas técnicas conocidas como técnicas de análisis y reingeniería de malware, pretenden facilitar la adquisición de conocimiento sobre el mismo de una manera sistemática y metodológica.

—*Desarrollo e implementación de una «honeynet»*, para obtener el estado del arte de los nuevos tipos de ataques y el conocimiento de sus vulnerabilidades, además de analizar cómo los nuevos escenarios de ataque se pueden incorporar en la metodología de pruebas de desarrollo y como afectan a la infraestructura de red, servidores de sistemas finales y a las aplicaciones críticas de usuario final.

Con el objetivo de poder realizar de forma práctica y experimental el análisis de malware se ha realizado un laboratorio y un estudio de las herramientas a utilizar en cada paso de la metodología de análisis propuesta. En la figura siguiente se muestra su arquitectura.

Figura 5. Diagrama laboratorio análisis malware



Además del estudio teórico de los métodos de análisis forense, se están realizando varios estudios de casos prácticos para lograr una mejor comprensión de los mecanismos internos de funcionamiento del malware y de las propias herramientas de análisis propuestas.

—Herramientas de acceso remoto (RATs).
—APT (Advanced Persistent Threat) orientado a la fuga de información

Conclusiones

1. La implantación de una *infraestructura de experimentación en Ciberdefensa* contribuiría al desarrollo de nuevas tecnologías innovadoras que aumentarían la disponibilidad, seguridad y viabilidad de las redes operacionales del Ministerio de Defensa y del entono civil, proporcionando verdadera protección cibernética.
2. La Unidad de Seguridad del ITM está creando en la actualidad, un Centro de Experimentación en tecnologías de

Ciberdefensa, abierto a una comunidad amplia de usuarios tanto del Ministerio de Defensa, como del entorno académico y/o las universidades, empresarial, como vía de coordinación de esfuerzos de investigación y desarrollo entre el entorno civil y militar.

3. Un aspecto importante de la seguridad del software es la confianza, sin embargo los desarrollos específicamente realizados para la FAS contienen fallos y vulnerabilidades de seguridad que potencialmente pueden ser explotadas por organizaciones maliciosas, en este sentido Unidad de Seguridad del ITM podría ayudar a incrementar la seguridad de las aplicaciones software, sistemas de información y mando y control mediante la aplicación de técnicas y herramientas de seguridad en la diferentes fase el ciclo de vida del software, en especial el análisis estático del código y dinámico.
4. Conocer la estructura, funcionamiento e interacción del malware, aportará una valiosa información, no sólo para el diseño y desarrollo de contramedidas eficaces, sino también para ayudar a conocer el origen de un ataque y la capacidad de evaluar si los sistemas del Ministerio de Defensa son capaces de detectarlo y por tanto tomar las acciones de respuesta necesarias y adecuadas.

Anexo I: Abreviaturas y Acrónimos

APT: Malware del tipo Advanced Persistent Threat.
CD&E: Desarrollo y experimentación de conceptos.
DDoS: Ataques de denegación de servicio distribuido.
DMZ: Zona desmilitarizada. Arquitectura de protección de accesos a redes de menor clasificación.
CCN: Centro Criptológico Nacional.
CIS: Sistemas de comunicaciones y de información.
DMZ: Zona desmilitarizada.
DNS: servidor de nombres
FAS: Fuerzas Armadas.
FFT: Sistemas de seguimiento de fuerzas amigas.
JEMAD: Jefe del Estado Mayor de la Defensa.
ISR: Sistemas de inteligencia, vigilancia y reconocimiento.

ITM: Instituto Tecnológico «La Marañosa».
MINSDEF: Ministerio de Defensa.
NEC: Network Enable Capability.
NINE: Network and Information Infrastructure (NII) Internet Protocol (IP) Network Encryption.
OTAN: Organización del Tratado del Atlántico Norte.
RATs: Herramientas de acceso remoto.
RDSI: Red Digital de Servicios Integrados.
SCIP: Protocolo de interoperabilidad de Comunicaciones Seguras.
SIP: Sesión Inition Protocol.
SSH: Secure Shell.
TIC,s: Tecnologías de la Información y la Comunicación.
VPN: Redes privadas virtuales.
VLAN: Redes de área local virtual.

Referencias

[1] Cuadernos de Estrategia 149. Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en ll Ciberespacio. Instituto Español de Estudios Estratégicos, Instituto Universitario «General Gutiérrez Mellado». Diciembre 2010
[2] Documento Informativo del IEEE 09/2011. Nuevo Concepto de Ciberdefensa de la OTAN (marzo de 2011).
[3] Design of the DETER Security Testbed. USC Information Sciences Institute University of California at Berkeley McAfee Research. Version: 27 May 2004.
[4] Build Your Own Security Lab. A Field Guide for Network Testing Michael Gregg. Published by Wiley Publishing, Inc. ISBN: 978-0-470-17986-4.
[5] CIS Security (Including Cyber Defence) Capability Breakdown. Autores: Geir Hallingstad, Luc Dandurand
[6] http://es.wikipedia.org/
[7] Open Framework for the NATO Secure Voice Strategy. Klaus-Dieter Tuchs, Ricardo Berto-Monleon,Hermann Wietgrefe (NATO Consultation, Command and Control Agency (NC3A)), Ammar Alkassar, Timm Korte (Sirrix AG security technologies).
[8] Malware Analyst's Cookbook and DVD Tools and Techniques for Fighting Malicious Code. Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard.

[9] Juan Ramón Bermejo Higuera. Trabajo Fin de Máster: Estudio de Técnicas Automáticas de Análisis de Vulnerabilidades de Seguridad en Aplicaciones Web. Año 2011.
[10] Estado Mayor de la Defensa (visión del JEMAD de la Ciberdefensa Militar. Año 2011.

Parte IV
EL CAMINO HACIA LA CIBERSEGURIDAD INTEGRAL EN ESPAÑA

CONTRIBUCIÓN DEL SECTOR EMPRESARIAL A LA CIBERDEFENSA

Ricardo Serrano Flores [*]

Cuestiones previas

La evolución del conocimiento tecnológico y más concretamente, en el sector de las comunicaciones, viene experimentando unos avances que siguen una línea más que exponencial. Es difícilmente comparable el tiempo transcurrido desde la invención de la imprenta hasta la aparición de los primeros ordenadores, con el tiempo trascurrido desde la aparición del primer teléfono móvil hasta nuestros días; en los que la mayoría de los smartphone o tablet que manejan nuestros hijos disponen de capacidades de proceso infinitamente superiores a los ordenadores de las década de los años 70; y apenas han pasado 30 años. Recuerdo mi primer teléfono móvil, pesaba casi un kilo, prácticamente no tenía cobertura, ...y curiosamente: «solo servía para hablar».

Para el año 2016, algunos analistas prevén que habrá 760 millones de tabletas en uso distribuidas por todo el mundo y 1.000 millones de personas poseerán un teléfono inteligente.

Cabe recordar asimismo el alto porcentaje de funcionarios públicos, incluidos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de las Fuerzas Armadas (FAS) que emplean por motivos laborales tanto su móvil de trabajo como el personal.

[*] Ricardo Serrano Flores, es Ingeniero Industrial, Presidente del Grupo *Voice Consulting* y Oficial Reservista Voluntario con experiencia en el Mando de Adiestramiento y Doctrina del Ejército de Tierra.

Del mismo modo la capacidad de relación, comunicación humana y acceso al conocimiento; han experimentado unos cambios y avances difícilmente imaginables hace unas décadas. Ahora podemos apreciar como a nivel personal y/o empresarial, estamos sustituyendo buena parte de la comunicación hablada por la comunicación escrita. Ahora nos relacionamos utilizando el Ciberespacio, y en este nuevo espacio de relación la cantidad de datos de todo tipo incluida voz, imagen, sonido, ...la ponemos a disposición de nuestros clientes, familiares, amigos, conocidos,... y «desconocidos» con una facilidad y muchos casos tranquilidad inusitada.

El fraude

Si bien las pérdidas económicas debidas al fraude en el Ciberespacio, son de escasa cuantía: aproximadamente el 80% son menores a 400€ la mayoría de los usuarios que lo han sufrido declaran haber sufrido pérdidas inferiores a 100€.

Dadas estas escasas cuantías, en muchos casos el fraude pasa inadvertido a la victima y por tanto no es denunciado. Aun en el caso de denuncia nos encontraríamos con que el código penal español lo trataría como una falta y no como un delito.

Peor aun es el caso en el que se accede a nuestra información, ya sean datos médicos, financieros, o cualquier otro de índole personal sin que seamos concientes de ello. Se da el caso de que solo tenemos control o prestamos atención, al acceso no deseado, cuando se produce un movimiento de dinero, pero ¿Cómo controlamos si alguien está accediendo, por ejemplo, a nuestros movimientos bancarios con el solo fin de obtener información, …?, lo mismo ocurre con nuestras agendas, contactos telefónicos, geoposición, llamadas o conversaciones telefónicas, …

Si nos centramos en la banca, solo el 75% de los usuarios de los nuevos canales de comunicación de las entidades financieras con sus clientes, reconoce vigilar asiduamente los movimientos de sus cuentas y solo comprueban el uso de una conexión segura a Internet cuando realizan un pago o transferencia por este canal el 70% de los consultados. Con todo, el nivel de confianza de los usuarios en el canal Internet es superior al 60%.

Hay que tener en cuenta que, en estos momentos, la mayor oficina de cualquier entidad financiera se encuentra en Internet. A lo largo de los últimos 5 años el número de operaciones y consultas que los usuarios realizan a través del ciberespacio es muy superior al realizado a través de la red de oficinas, dándose el caso en el que un gran número de usuarios no tiene necesidad de acudir nunca a una oficina. Pues bien, cualquiera que consulte los movimientos de la cuenta donde tiene domiciliados la mayoría de sus recibos y pagos, se encontrará con que también aparecen movimientos de pequeñas cantidades cuyos conceptos corresponden a comisiones, gastos de mantenimiento, …

Estos movimientos en la mayoría de los casos son asumidos como normales y no se les presta demasiada atención si se producen ocasionalmente y las cantidades están por debajo del euro o apenas lo superan; pero hay que tener en cuenta que los «piratas informáticos», para no ser detectados, realizan este tipo de cargos muchas veces a un gran número de distintos clientes y las «ganancias» obtenidas son considerables.

No entraré en la descripción de los distintos medios y formas por las que un delincuente consigue acceder a nuestra información en el ciberespacio, lo que si apuntaré es que cada día hay una nueva versión y cada vez es más sofisticada.

Lo descrito para el sector financiero lo podemos extender a cualquier otro ya que cada día accedemos a los servicios que prestan las empresas o la administración a través de los denominados nuevos canales de comunicación. En todos los casos, es evidente, que un usuario puede llegar a detectar con cierta facilidad un fraude que suponga un movimiento de dinero; lo complicado es llegar a saber que alguien está accediendo a nuestra información sin nuestro permiso o lo que es más complicado: llegar a conocer el uso posterior que se dará a la información.

Cuando se accede a cualquier sistema sin el permiso y conocimiento de su legal usuario los daños que se puedan llegar a producir muchos especialistas los están llegando a comparar con los producidos por los accidentes nucleares; pongamos el ejemplo de un ataque a cualquiera de las infraestructuras críticas del país y por ser más concreto me referiré a los sistemas de cloración del agua de una gran ciudad; en determinadas circunstancias de

tiempo y lugar nos podemos encontrar con un problema sanitario de consecuencias extremas.

Llegados a este punto, hay que hacer especial mención a los dispositivos de telefonía móvil que ya en estos momentos disponen de gran capacidad de proceso y almacenamiento y que en un futuro no muy lejano sustituirán completamente a los ordenadores personales tal y como los conocemos hasta ahora. En nuestros teléfonos móviles solemos almacenar todo tipo de información personal y confidencial: agenda, contactos, fotos, direcciones, claves,…y aplicaciones que instalamos y a las que les damos permiso de acceso a toda esa información sin ningún tipo de control.

Pues esto no es lo peor; lo más complicado y a la vez sencillo de entender es que un teléfono móvil, como su propio nombre indica, es un teléfono que nos lo podemos llevar a todas partes y que para la mayor parte de nosotros se ha convertido en un compañero inseparable a nivel personal y profesional, cuando no en una herramienta de trabajo o de ocio propiamente dicha; y aquí está el problema: hablamos desde cualquier sitio y a cualquier hora, ya estemos en una reunión de trabajo, familiar, personal,… y la mayoría de los nuevos dispositivos conocen nuestra posición, donde estamos o donde no estamos, y pueden contener aplicaciones ocultas que envían no solo nuestra posición sino nuestra llamadas, mensajes, o ¿ porqué no ¿, las grabaciones vocales del contenido de nuestras conversaciones. Pondré el simple ejemplo de una persona que quiere controlar lo anteriormente descrito en uno de sus empleados, sus hijos o su pareja sentimental,… solo tendría que instalar, o hacer instalar, un sencillo «programa oculto» en su smartphone.

Hay que tener en cuenta, también, que empresas e instituciones pueden llegar a utilizar «maliciosamente» las posibilidades que ofrece el ciberespacio; en este caso hablo de ciberespionaje con fines empresariales, económicos o institucionales,…

La capacidad tecnológica y la formación

A nivel nacional, son pocas las compañías con capacidad para fabricar los elementos físicos que componen las estructuras «complejas» del denominado ciberespacio, me refiero a lo que llamamos Hardware: ordenadores, routers, sistemas de telefonía, … por no decir satélites de comunicación. En el caso de los lenguajes

de programación o sistemas de desarrollo, lo que denominamos Software, nos encontramos con que los grandes «standards» también pertenecen a compañías multinacionales.

Otra cosa son las aplicaciones, o la integración de sistemas para configurar otros más complejos; en este caso y más concretamente en el desarrollo de aplicaciones y en el conocimiento de los sistemas relacionados con el ciberespacio disponemos de expertos que están al mismo nivel de los países más avanzados. El problema es que en cualquier parte del mundo nos podemos encontrar con un gran número de personas que disponen del conocimiento necesario para el desarrollo de aplicaciones «maliciosas» y su implantación en el ciberespacio y los sistemas que lo componen y configuran.

Es tal el desarrollo que está adquiriendo el ciberespacio, nuestra relación diaria con dicho espacio donde se almacena y distribuye el conocimiento y su necesidad de utilización para nuestra actividad profesional, personal y de ocio que gran cantidad de personas, incluso sin titulación técnica, poseen conocimientos suficientes como para interactuar, desarrollar, mantener,… con sistemas y aplicaciones.

A nivel empresarial, cada vez más, se están incorporando a nuestros departamentos de desarrollo de sistemas o incluso de I+D, personal con distintas titulaciones que no son técnicas y con formación adquirida de forma autodidacta, pero a los que su iniciativa e inquietud profesional les ha dirigido hacia el mundo de la informática aplicada a los sistemas y desarrollos relacionados con Internet. Además, a nivel universitario o desde la formación profesional los nuevos titulados cada vez disponen de mejores conocimientos relacionados con el sector, dándose casos de personas con capacidades muy importantes, incluso, durante sus etapas de formación sin ni siquiera haber accedido al mercado laboral.

Esto quiere decir que, no solo en los países de nuestro entorno sino a nivel prácticamente mundial, nos podemos encontrar con personas que bien formando grupos de trabajo coordinado o incluso a nivel particular y desde sus propias casas pueden crear y crean aplicaciones llamémoslas de «dudosa intención».

Por tanto, la preocupación en empresas e instituciones por la ciberseguridad y la ciberdefensa, en estos momentos, es más

acuciante. Desde las empresas se están adoptando todo tipo de soluciones para salvaguardar sus sistemas y la confidencialidad de los datos propios y de clientes; lo mismo ocurre con las instituciones que, además, tienen que velar por el correcto mantenimiento de sus infraestructuras propias o que dan servicio a los ciudadanos. Esta preocupación hace necesario cada vez más personal correctamente formado en la seguridad técnica e informática y por tanto abre nuevas posibilidades a empresas y profesionales que se dedican a este sector. Curiosamente, y es conocido, que las mejores empresas tratan de contratar a los mejores profesionales que en muchas ocasiones tenían ocupaciones «no tan profesionales». En otros casos se recurre, incluso mediante concursos o competiciones, a premiar y seleccionar al profesional que ha sido capaz de «violar» un sistema o aplicación determinada.

Si lo que preocupa es la seguridad nacional tendríamos que, no solo que hablar de sistemas o aplicaciones, sino de unidades de los cuerpos y fuerzas de seguridad o incluso del ejercito, plenamente dedicadas tanto a la ciberdefensa como al ciberataque. En países como EE.UU. o Inglaterra se están invirtiendo importantes cantidades de dinero en la formación y preparación de unidades militares plenamente dedicadas tanto a la defensa como a la guerra en el ciberespacio.

Contribución empresarial a la ciberdefensa

Si tenemos en cuenta, como ya he indicado, que es el sector financiero donde históricamente se vienen produciendo los mayores porcentajes de «ataques» a los sistemas e información con fines fraudulentos; entenderemos que es en este sector donde se concentra la mayor inversión para tratar de protegerse en el ciberespacio. Además, día a día, la presencia e importancia de buena parte del negocio financiero se gestiona en este nuevo espacio de relación y comunicación entre empresas, clientes y usuarios de los servicios.

Empresas e instituciones, han tenido y tienen la necesidad de contar con personal preparado; este personal en algunos casos forma parte de las propias plantillas, pero es también frecuente la externalización de estos servicios de protección ante amenazas cibernéticas. En los últimos 10 años han surgido, a nivel nacio-

nal, varias empresas con un alto grado de especialización en la «contención» del fraude en el ciberespacio, dándose el caso de que la preparación de sus profesionales es superior a la de los profesionales con que cuentan las fuerzas de seguridad, además, hay que tener en cuenta que el número de personas preparadas en el sector empresarial es muy superior.

En cuanto a la protección de los datos la I+D de las empresas especializadas se está centrando en avanzar en sistemas y aplicaciones relacionadas con la encriptación de la información, o en desarrollos relacionados con la utilización de información biométrica que viaje por canales alternativos a los utilizados. Pero también la protección en este nuevo canal se centra en la formación de los usuarios, formación dirigida hacia la autoprotección haciendo ver al usuario los riesgos del canal.

Cuando nos referimos a la ciberdefensa nacional, lo más importante se centra en la protección de las infraestructuras críticas del país, entre las que se encuentran los sistemas controlados por las FAS. En este sentido, es importante, que nuestro país disponga de unidades militares altamente especializadas en ciberdefensa, ciberdefensa que ha de contar entre sus prioridades con la ciberinteligencia. Ante un ataque cibernético, venga de donde venga; ya he comentado que una sola persona o un pequeño equipo con la suficiente preparación puede ocasionar un «terrible» contratiempo,… en estos casos, y en cualquier otro, lo importante es adelantarse al «ataque», conocerlo con antelación para poder prevenirlo antes de que ocurra, ya que una vez se haya producido, en la mayor parte de los casos, la marcha atrás será inviable.

La experiencia empresarial en casos de ciberataques a entidades financieras nos dice que la inversión en medidas de protección es siempre muy inferior a los costes derivados de los daños producidos. Al menos en estas entidades, la jurisprudencia está haciendo casi siempre responsable a la entidad frente al daño producido al cliente, no digamos ya cuando el daño se le produce directamente a la entidad e incide sobre un gran número de clientes.

Si trasladamos el ejemplo a la seguridad nacional nos encontraremos con los mismos efectos: la inversión en prevención será siempre muy inferior a los costes de reparación de los daños

producidos. Esto que es así en la mayoría de los casos de la vida, s e trate de lo que se trate; en el caso de las amenazas ciberneticas cobrará una mayor importancia según pase el tiempo y la utilización del ciberespacio se generalice todavía más.

Las futuras unidades de Ciberdefensa de las FAS, desde mi punto de vista, han de ser unidades en las que se impliquen y se vean reflejados los intereses de defensa a nivel público y privado. Han de ser unidades con personal militar altamente especializado en ciberdefensa y donde la ciberinteligencia ocupe un lugar prioritario, pero también han de contar con la permanente colaboración de las empresas especializadas a nivel nacional; estas empresas o instituciones además de universidades o centros de formación especializados, han de contar con personal que pueda integrarse fácilmente dentro de la estructura orgánica de las unidades militares en caso de crisis y que en cualquier caso trabaje en permanente colaboración con dichas unidades. Obvia comentar que quien sabe defenderse adecuadamente, también conoce como realizar un adecuado ataque, y este caso los medios y materiales necesarios serían los mismos.

Conclusiones

Si las comunicaciones han sido a lo largo de la historia un motor para el desarrollo de nuestra sociedad y un medio por el cual los humanos nos relacionamos. El control de las vías y medios de comunicación, también, ha sido una prioridad para los estados, sus instituciones y empresas. Del mismo modo los ataques a los medios que hacen posible las comunicaciones, sean del tipo que sean, han sido una de las prioridades en caso de conflicto.

Con los desarrollos tecnológicos que han hecho posible la aparición de la comunicación a través del ciberespacio y la cada vez más frecuente conexión de cualquier sistema o dispositivo a esta nueva vía de comunicación y por tanto relación; el tipo de amenazas sobre la confidencialidad de información transmitida o sobre la integridad, correcto y legal funcionamiento de las infraestructuras conectadas se hace cada vez más impredecible; fundamentalmente por la facilidad en cuanto a medios para realizar ataques y la adquisición de competencias para realizarlos.

Cada vez, queda más claro que una vez perpetrado un ataque exitoso, la reacción siempre llegará tarde y que por tanto la prevención y la inversión que se realice a la hora de prevenir, en todos los casos, será inferior al daño producido.

En el caso de la defensa a nivel nacional, se trata de organizarla de forma que participen activamente las FAS en conjunción con el resto de instituciones, organismos y empresas especializadas. Se trataría de crear un nuevo quinto ejercito para un nuevo espacio de actuación con la preparación necesaria para actuar en un particular teatro de operaciones, el Ciberespacio.

En cualquier caso, todo el esfuerzo realizado en este sentido, siempre repercutirá en beneficio del resto de la sociedad ya que la I+D+i derivada de los esfuerzos en la ciberdefensa serán aplicables a avances en las tecnologías y sistemas de comunicación.

PRIORIDADES NACIONALES EN CIBERSEGURIDAD

Javier Candau Romero [*]

Introducción

En los últimos años se ha detectado un incremento constante de vulnerabilidades y amenazas sobre los Sistemas y Tecnologías de la Información y Comunicaciones. Estas amenazas, que no tienen por qué ser deliberadas (los errores y omisiones del personal autorizado y bienintencionado pero desconocedor de buenas prácticas de seguridad también lo son), evolucionan continuamente y representan un verdadero desafío para los responsables de proporcionar servicios electrónicos.

En el caso de las amenazas voluntarias, el reto es aún mayor si tenemos en cuenta que aquellos que intentan infiltrarse o explotar nuestros sistemas emplean recursos mejores y más sofisticados. Además, en la actualidad los ataques se pueden llevar a cabo desde cualquier parte del mundo y, en muchos casos, las posibilidades de descubrir su origen, e incluso su presencia, son muy remotas por lo que es necesario un esfuerzo de todos para intentar abordar este problema.

Con el desarrollo de las tecnologías de comunicaciones, se ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios han eliminado las barreras de distancia y tiempo. En el nuevo espacio relacional —el ciberespacio—, se han diluido las fronteras nacionales y, a la vez, se ha producido un considerable aumento de las posibilidades pero también de

[*] Javier Candau Romero es Teniente Coronel del Ejército de Tierra, Jefe del Área de Ciberamenazas del Centro Criptológico Nacional.

las amenazas, acrecentadas éstas por el constante crecimiento de la dependencia cibernética de las sociedades avanzadas.

Este hecho se agrava con la excesiva uniformidad de los medios empleados (TCP/IP, Windows, Web ...) que facilitan la rentabilidad de la formación de los atacantes y el impacto global de la explotación de las vulnerabilidades y los fallos detectados. En definitiva la superficie de ataque es inmensa

Por ello, ningún sistema, incluidos todos los de la Administración, está a salvo de sufrir un ataque de graves consecuencias como el robo, pérdida, destrucción o extracción de dispositivos de almacenamiento; destrucción o modificación de datos almacenados; redirección de Información para usos fraudulentos; interceptación de datos mientras se procesan, correo no deseado, etc.

Los ciberataques normalmente comparten las siguientes características comunes:

Bajo coste. Muchas herramientas de ataque se pueden descargar de forma gratuita o con un coste muy bajo para el daño que pueden causar.

Fácil empleo. Para muchos ataques no son necesarios grandes conocimientos técnicos. Existen herramientas con unos interfaces de usuario muy amigables y sencillas de usar.

Efectividad. Existe una probabilidad muy alta de alcanzar los objetivos buscados con estos ataques por la ausencia de políticas de empleo o la limitación de recursos existentes en la parte defensiva debido a la falta de concienciación de las organizaciones gubernamentales, empresas y ciudadanos.

Bajo Riesgo para el atacante. Es muy difícil atribuir un ataque con las herramientas de ocultación del origen existentes actualmente en Internet y por la diferencia de legislaciones de los diferentes países.

Además, algunos de los siguientes factores tecnológicos incrementan la posibilidad de estos ataques:

—La complejidad creciente de la tecnología hace más difícil determinar el grado de seguridad de un determinado producto o sistema.

—La rapidez de la evolución tecnológica y las exigencias y competitividad del mercado ocasionan que, con frecuencia,

se desplieguen productos con vulnerabilidades y fallos de seguridad que son aprovechados por los agresores.
—Existe un mayor riesgo en el caso de productos fabricados en países fuera de la órbita occidental, ya que es más difícil controlar la introducción de elementos inseguros.
—Hay una relativa falta de madurez de la industria de las tecnologías de la información y las comunicaciones, al no considerar la seguridad como un factor de diseño de los productos o sistemas.
—Se constata un constante incremento de la interconexión de todo tipo de sistemas utilizando Internet.

Existen evidencias de que determinados países tienen programas de capacitación técnica para lograr realizar ciberataques. En algunos casos, dicha capacitación técnica es considerada y abordada como una capacidad militar más con la que se plantean lograr la superioridad.

En un primer análisis sobre la situación global de la cibercriminalidad, puede afirmarse que las técnicas utilizadas son cada vez más depuradas y que existe una mayor interrelación entre los ciberdelincuentes de diversos países.

Muchos países han desarrollado o están desarrollando estrategias nacionales de Ciberdefensa con las que persiguen conseguir un ciberespacio más seguro mediante el intercambio de información de alertas, vulnerabilidades, amenazas y eventos; la mejora de las capacidades de contrainteligencia, la seguridad de sus productos y tecnologías, y la concienciación y formación de sus ciudadanos y servidores públicos en seguridad de sistemas de las Tecnologías de la Información y Comunicaciones (TIC).

Para ello, identifican los actores y responsabilidades presentes en un escenario de ciberseguridad, establecen unos principios comunes de actuación, proponen las líneas de acción para alcanzar como nación las capacidades necesarias de ciberdefensa y crean las estructuras de decisión y coordinación y los flujos de información necesarios para coordinar la prevención y respuesta ante los cibertaques.

Finalmente, en la mayoría de ellas impulsan el desarrollo de los sistemas de alerta y prevención adecuados que les permitan disponer de una visión de conjunto sobre este problema.

En España, durante los últimos 12 años se han desarrollado iniciativas parciales (criterios de seguridad, conservación y normalización, Centro Criptológico Nacional, infraestructuras críticas, Instituto Nacional de Tecnologías de Comunicación o esquema nacional de seguridad) que se pasaran a describir con las que se intenta mitigar el riesgo de recibir cualquier tipo de ataque procedente de este nuevo tipo de amenaza.

Agentes de la amenaza. Priorización

Actualmente, por su impacto en el ciberespacio, se destacan las siguientes manifestaciones:

—Otros Estados, Servicios de Inteligencia y/o Unidades cibernéticas de las Fuerzas Armadas: Se considera el principal vector de amenaza contra la información sensible o clasificada manejada por los sistemas de información gubernamentales y las empresas nacionales de sectores estratégicos (especialmente aquellas relacionadas con la Defensa). Estos atacantes disponen de medios y recursos técnicos y una gran capacidad de acción. Sus actividades son muy prolongadas en el tiempo y el tipo de herramientas que utilizan (APT [1]) normalmente muestran unos niveles muy bajos de detección en los sistemas de seguridad de los objetivos. Las unidades de las FAS. pueden ser un vector de amenaza crítico sobre todo en tiempo de crisis o conflicto pues tienen asignadas misiones de ataque a los sistemas de información de los adversarios.

—Espionaje industrial: Son compañías o gobiernos que tienen interés en disponer de información crítica respecto de desarrollos tecnológicos e industriales (propiedad intelectual o industrial) de empresas de la competencia. Esta actividad se solapa con el ciberespionaje protagonizado por los propios Estados. Su objetivo principal es la propiedad intelectual de empresas de la competencia.

1. APT. *Advanced Persistent Threat.* (Amenaza Persistente Avanzada).

—Crimen Organizado: El crimen organizado se ha introducido en el entorno digital, realizando actividades ilícitas relacionadas con el robo de información de tarjetas de crédito, certificados digitales asociados, con el fraude telemático asociado a operaciones bancarias, con el blanqueo de dinero, con la vulneración de los derechos de propiedad intelectual e industrial, con la pornografía infantil o con el robo de identidades asociado a inmigración ilegal, por poner tan solo algunos ejemplos.

—Hacking Político y/o Patriótico: Este tipo de actividad es el reflejo de un conflicto regional, étnico, religioso o cultural en el ciberespacio. Normalmente, no tiene un gran impacto en los sistemas de información del país atacado pues la actividad suele limitarse a ataques realizados contra servicios Web, no alcanzado los sistemas internos. Últimamente, la aparición de grupos como Anonymous, Luzsec o Antisec que incluyen entre las modalidades el robo de datos, hacen que esta amenaza haya alcanzado más importancia.

—Terrorismo. El uso del ciberespacio por parte de organizaciones terroristas y grupos radicales presenta una doble vertiente: en forma de instrumento para la comisión de actividades tales como propaganda, comunicaciones internas, difusión de manuales de entrenamiento, financiación, reclutamiento y obtención de información; y también como fin, haciendo uso del ciberespacio como objeto de los ataques. Todo ello conforma lo que se ha dado a conocer por Ciberterrorismo, que supone además una amenaza potencial que, tanto de forma aislada, como combinada con una acción terrorista convencional, puede llegar a interferir o anular el normal funcionamiento de alguno de los servicios esenciales proporcionados por las conocidas como Infraestructuras Críticas.

Algunos de estos agentes suelen contratar capacidades técnicas de ataque disponibles en el mercado negro ofertadas por hackers y organizaciones criminales si no disponen de la capacidad tecnológica necesaria y podrían, en su caso, manipular usuarios internos para disponer de la información o las credenciales necesarias con la

que acceder a los sistemas de información objetivos desde dentro. Se trata con un poco más de detalle el ciberespionaje.

Ciberespionaje

Los ciberataques más sofisticados se esperan de los servicios de inteligencia y las agencias de operaciones de información militares extranjeras. En la mayoría de los casos, estos atacantes disponen de muchos recursos, tienen la paciencia necesaria para encontrar la debilidad del sistema y durante la explotación del ataque intentan lograr la mayor persistencia en el mismo instalando puertas traseras en previsión de una posible detección del mismo.

El objetivo de estos ataques es el mismo que la actividad de inteligencia que lo soporta, adquirir ventaja política, económica, comercial o militar con la información adquirida en los sistemas atacados.

Todos los estados del primer mundo que soportan sus actividades en sistemas de información y que necesitan la interconexión con Internet para alcanzar mayores cotas de eficiencia son susceptibles de recibir este tipo de ataques que intentan alcanzar la información clasificada o sensible, información privada de alto valor o secretos industriales.

Muchos Estados han declarado públicamente que el ciberataque puede ser empleado como una herramienta más de sus estrategias de inteligencia o militares. En este sentido su objetivo final es tanto la ex filtración (compromiso) de información del enemigo como la inutilización o destrucción de los sistemas enemigos tanto para evitar el mando y control de sus fuerzas como para causar daños en sus servicios esenciales y en su población.

La constatación clara de esta realidad es que en los últimos años se han detectado numerosos intentos de agresión, muchos de ellos exitosos, sobre sistemas sensibles de diferentes naciones en el ámbito de la UE y la OTAN. Todas las naciones de la UE y OTAN han declarado públicamente haber recibido ataques muy graves con impactos serios sobre la información sensible manejada en los sistemas de sus respectivos gobiernos. Seguramente muchos otros gobiernos y empresas han recibido ataques similares que no se han hecho públicos.

Por ello se cree imprescindible la protección de estos sistemas contra ciberataques interesados en la información manejada por los mismos. Esta protección debe preservar tanto la confidencialidad de esta información como la disponibilidad e integridad de ésta. Una de las actividades críticas a realizar por las diferentes administraciones es incrementar las actividades de monitorización, detección y eliminación de estas agresiones que normalmente requiere un incremento notable en los presupuestos asignados a seguridad.

Asimismo se deben regular las salvaguardas a implementar según el nivel de la información manejada por los sistemas para que el perímetro de protección de todos los sistemas de la administración sea homogéneo y la dificultad a la que se enfrente el atacante sea similar independientemente del organismo al que ataque.

Se deben realizar las mismas actividades en los sistemas de empresas que se consideren estratégicas pues el nivel de amenaza es similar.

En conclusión, el ciberespacio ha reducido la dificultad de entrar en el juego del espionaje y el crecimiento de Internet incrementa la superficie de actuación, por ello, la posibilidad de recibir ataques procedente de otros estados intentando adquirir información sensible o clasificada de su gobierno, información de sus empresas estratégicas es quizás el riesgo más elevado al que se enfrentan las naciones,

Infraestructuras críticas

Desde hace una década la seguridad de las infraestructuras críticas vienen ocupando la agenda de los responsables políticos en todo el mundo como un aspecto estratégico para garantizar la propia seguridad de nuestros países y nuestros ciudadanos.

Las Infraestructuras críticas, según se definen en la legislación correspondiente [2] es el conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica,

2. Véase www.cnpic.es. Fecha de consulta 11 de octubre de 2012.

de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación.

Este impacto se mide según unos criterios horizontales que determinan la criticidad de una infraestructura. Se han establecido tres:

—el **número potencial de víctimas** mortales o de lesiones graves que pueda producir;
—el **impacto económico** en función de la magnitud de las pérdidas económicas y/o el deterioro de productos o servicios, incluido el posible impacto medioambiental;
—el **impacto público**, por la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

Las infraestructuras críticas se agrupan en 12 sectores entre los que se incluyen la Administración, el sector aeroespacial, el sector energético, el de la industria, el nuclear, el de la industria química, las instalaciones de investigación, el de agua, el de la salud, el de transporte, el de alimentación, el financiero y tributario y el de las tecnologías de la información y comunicaciones [3].

Centro Nacional de Protección de Infraestructuras Críticas

La Secretaría de Estado de Seguridad (SES), es el órgano responsable de la dirección, coordinación y supervisión de la protección de infraestructuras críticas (PIC) nacionales, de la creación del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC [4]), como órgano director y coordinador de dichas actividades, y de la determinación, clasificación y actualización del Catálogo de Infraestructuras críticas.

3. Véase Anexo legislación Protección de infraestructuras críticas: sectores estratégicos y ministerios / organismos del sistema competentes en su protección.

4. Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). http://www.cnpic-es.es/

Las funciones principales del CNPIC son las de coordinar la información y la normativa; convertirse en el punto de contacto permanente con los gestores, tanto públicos como privados, de las infraestructuras críticas; dirigir y coordinar los análisis de riesgos; establecer los contenidos mínimos de los planes de seguridad de operador (PSO) y de los planes de protección específicos (PPE) de las infraestructuras críticas; establecer un sistema de mando y control y actuar como punto de contacto con centros similares en todo el mundo.

La normativa tiene como objetivos principales dirigir y coordinar las actuaciones en materia de protección de Infraestructuras Críticas, previa identificación y designación de las mismas, impulsando, además, la colaboración e implicación de los organismos propietarios de dichas infraestructuras a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo.

Catálogo y Plan de Infraestructuras Críticas

Este catálogo está clasificado de Secreto, registra las infraestructuras consideradas como críticas y que, en su caso, requieren de especiales medidas de protección. Actualmente existen unas 3.000 infraestructuras críticas, de las que el 80% de ellas pertenecen al sector privado. Asociado a cada infraestructura, esta base de datos especifica las medidas de protección, los planes de reacción y la criticidad de la misma.

Es la herramienta fundamental de trabajo pues además de almacenar toda la información sobre la infraestructura establece el punto de enlace con los operadores, fuerzas y cuerpos de seguridad del Estado (FCSE) y cualquier otro representante del sistema de protección de infraestructuras críticas. Permite la actualización continua y facilita el proceso de la evaluación de la criticidad y del nivel de seguridad de las infraestructuras evaluadas por el CNPIC.

Cualquier estrategia de seguridad en estas infraestructuras debe tener como uno de sus elementos centrales prevenir posibles ataques, disminuir la vulnerabilidad y, en el caso de que se produjeran situaciones de crisis que afectaran a las infraestructuras esenciales, minimizar los daños y el periodo de recuperación.

Esta estrategia es el Plan Nacional de Protección de Infraestructuras Críticas en el que se establecen los criterios y las direc-

trices precisas para movilizar las capacidades operativas de las Administraciones públicas y para articular las medidas preventivas necesarias, con el fin de asegurar la protección permanente, actualizada y homogénea del sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

Además establece que se articulen unos planes estratégicos sectoriales basados en un análisis general de riesgos que contemple las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten a cada sector.

A partir de estos planes, cada operador debe articular los planes de Seguridad del Operador (PSO) y los planes de protección específicos (PPE) de sus infraestructuras críticas que asociado al análisis de riesgos de la instalación o sistema, establecerán la adopción de medidas permanentes de protección y de medidas temporales y graduadas, en razón a la amenaza específica que se detecte en cada momento (tanto físicas como de carácter lógico).

La elaboración de esta documentación se encuentra actualmente en su fase inicial y será necesaria una mayor publicación de esta normativa de desarrollo para poder definir de una forma clara los requisitos mínimos de seguridad que deben cumplir las mismas.

Ciberataques en las infraestructuras críticas

El borrador de legislación se centra especialmente en contemplar, evitar o minimizar los ataques físicos a las infraestructuras críticas; la única referencia disponible en el borrador a ciberataques es la plasmada en la realización del análisis de riesgos y en la redacción de los planes de protección específicos de las infraestructuras críticas donde se contemplan las amenazas lógicas.

Será necesario un desarrollo del mismo donde se contemplen con mayor detalle las amenazas y vulnerabilidades de estas infraestructuras relacionadas con el ciberespacio pues en la actualidad todas las consideraciones de detalle están centradas en ataques físicos (en su mayoría de carácter terrorista) sobre las mismas.

En otros países se contempla con mucha mayor profundidad la posibilidad de estos ataques identificándolos como un asunto crítico a tratar.

Los ciberataques se plantean con especial criticidad en el sector de Tecnologías de Información y Comunicaciones y en los sistemas de información y comunicaciones que soportan otros sectores estratégicos como los de la Administración y los sistemas SCADA (Supervisory Control And Data Acquisition, Sistemas de Control de Procesos).

Sistemas SCADA

En muchos de los sectores estratégicos nombrados, para supervisar y mantener el control de las infraestructuras se utilizan sistemas de control, llamados comúnmente SCADA.

Así, con los sistemas SCADA se controlan los procesos de fábricas químicas, redes eléctricas, centrales de generación eléctrica, industrias de petróleo y gas, tratamiento de agua y residuos e industrias farmacéuticas entre otros.

Hasta hace poco, el relativo desconocimiento de este tipo de sistemas reducía al mínimo sus riesgos de seguridad. No obstante, ya en 2005 se anunció la primera vulnerabilidad de un sistema de control, generando un gran debate acerca de la divulgación de dicha información. Desde entonces, el interés en los sistemas de control industrial ha crecido exponencialmente, en parte como consecuencia de la conexión de éstos con redes de comunicaciones públicas (Internet) y por la incorporación de tecnologías comerciales (equipos de comunicaciones o sistemas operativos entre otros) para maximizar la rentabilidad de las inversiones.

En 2008 aparecieron los primeros programas diseñados para explotar las vulnerabilidades de los sistemas de control industrial. En 2009 y 2010 se han detectado ataques a estos sistemas.

El riesgo principal de estos sistemas es el desconocimiento por parte del propietario de las interconexiones reales de los sistemas SCADA, la ausencia de buenas prácticas de seguridad como la realización de actualizaciones periódicas o una adecuada gestión de las contraseñas y las deficiencias en la configuración de los diferentes dispositivos que proporcionan muchas posibilidades de realizar acciones remotas que permiten el control de los mismos.

Conclusiones estratégicas nacionales de ciberseguridad

En este apartado se muestran las conclusiones derivadas del análisis de estrategias de seguridad publicadas oficialmente siempre desde el punto de vista defensivo. Estos documentos, en sus versiones públicas, no tratan el aspecto ofensivo del ciberespacio y no se analizarán en este apartado.

Se presentan las conclusiones de las aproximaciones de las naciones que han presentado públicamente las soluciones para abordar este problema:

—Estrategia de Ciberseguridad en Estados Unidos [5] publicada en 2003.

—Estrategia de Ciberseguridad en el Reino Unido [6] fue publicada en junio de 2009.

—Estrategia de Ciberseguridad en Canadá [7] fue publicada en 2010.

—Estrategia francesa sobre ciberseguridad se establece el libro blanco de la seguridad y Defensa Nacional [8] aprobado por el Presidente de la República en junio de 2008.

—Estrategia de Ciberseguridad en Alemania [9] publicada en febrero de 2011.

—Estrategia de Ciberseguridad en Paises Bajos [10] publicada en junio de 2011.

—Estrategia de seguridad de Estonia publicada en mayo de 2008 [11].

5. Véase http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

6. Véase Cyber Security Strategy of the United Kingdom. June 2009. Cabinet Office. www.cabinetoffice.gov.uk

7. C Véase anada´s Cyber Security Strategy http://www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.aspx

8. Véase Livre blanc sur la défense et la sécurité nationale. http://www.livreblancdefenseetsecurite.gouv.fr/information

9. Véase Cyber Security Strategy for Germany. Febrero 2011 www.bmi.bund.de

10. The National Cyber Security Strategy (NCSS). Junio 2011. Ministerio de Seguridad y Justicia

11. Véase Cyber Security Strategy for 2008-2013. Cyber Security Strategy Committee. Ministry of Defence. ESTONIA. Tallinn 2008. http://www.mod.gov.ee/en/national-defense-and-society

—Estrategia de seguridad de Australia publicada el 23 de noviembre 2009 [12].
—Aproximaciones a la ciberseguridad en OTAN y UE.

Del análisis de estas estrategias se extraen las siguientes conclusiones:

—Se realiza una aproximación global al problema tratando de forma conjunta todos los niveles sobre los que se debe actuar en ciberdefensa:
  • Gobiernos centrales, regionales y locales.
  • Empresas y tejido industrial
  • Infraestructuras críticas
  • Fuerzas y cuerpos de seguridad del Estado
  • Ciudadanos
—Se reconoce que es un problema emergente, que el escenario es incierto, que es una de las prioridades para la seguridad nacional y como tal, se debe abordar.
—En las naciones analizadas, se centralizan las responsabilidades en ciberdefensa en uno o dos organismos o en un una oficina de coordinación cuya dependencia es del presidente o primer ministro o, en su caso, se fortalece de forma explícita la posición de los organismos a los que se asigna esta misión.
—Se potencian las capacidades de monitorización y alerta temprana, se concentran y se fortalecen los equipos de respuesta ante incidentes (especialmente las gubernamentales) por considerarlos los mejor posicionados para resolver el problema de las nuevas amenazas de forma más eficiente.
—Se impulsan esquemas nacionales de seguridad (requisitos de seguridad mínimos a implantar en las redes gubernamentales) y se intentan disminuir las interconexiones con Internet.
—Se priorizan y fortalecen las capacidades de inteligencia por el mejor conocimiento que poseen de la amenaza con el objetivo de hacer frente a ataques complejos.

12. Véase Cyber Security Strategy. http://www.ag.gov.au/cybersecurity

—Se declara como necesidad estratégica la formación y concienciación de servidores públicos, empresas y ciudadanos. Se presentan diversas soluciones para conseguir este objetivo.
—Se impulsan las actividades de investigación e innovación en este campo mediante alianzas con Universidades y centros de investigación.
—Se proporciona una dotación presupuestaria para la implantación de las estrategias con la vocación política de mantenerla en el tiempo.

En el siguiente cuadro se adjuntan estas conclusiones:

Figura 1

Componente o Política de la Estrategia	Objetivos e Indicador de la Actividad
Consideración de la Ciberseguridad como un asunto de Seguridad Nacional	Resulta absolutamente prioritaria la formulación de políticas globales e integradas, que aglutinen a todas las áreas gubernamentales concernidas, designando la autoridad responsable de su coordinación al más alto nivel posible.
Arquitectura Institucional Formal	Creación y fortalecimiento de las organizaciones con responsabilidades en materia de ciberseguridad, definiendo y delimitando sus funciones y roles y asignando los recursos precisos: presupuestarios y humanos. Las instituciones clave incluirán: 1) Coordinador de la política de ciberseguridad, al más alto nivel 2) Centro de coordinación operacional y 3) Centro de respuesta a incidentes
Desarrollo de Capacidades y Conocimientos especializados	Necesidad de adoptar "nuevos" enfoques para la ciberseguridad, que deberán centrarse en el desarrollo y/o fomento de instituciones educativas y programas de formación que vengan a satisfacer la demanda de personal especializado, así como la determinación de los presupuestos precisos para fomentar la seguridad del sector TIC nacional.
Dependencia especial de la Comunidad de Inteligencia	Tendencia significativa en la mayoría de los países para que las agencias de inteligencia o las unidades de inteligencia militar puedan, de facto, ganar influencia en la orientación general de la ciberseguridad.
Protección de infraestructuras críticas	Desarrollo o mejora de los esfuerzos para proteger los componentes TIC de Infraestructura Crítica nacionales, lo que implica la identificación y categorización de estas infraestructuras y la asignación de responsabilidad a una autoridad nacional de seguridad.
Coordinación público-privada	Incremento de las medidas para armonizar los esfuerzos del sector privado en materia de ciberseguridad con los planes gubernamentales de ciberdefensa, medidas que pueden ir desde la cooperación informal, a la institucionalización de la cooperación, a través de propuestas regulatorias y normativas.
Alcance Internacional	Incremento de los esfuerzos de muchos países con intereses comunes para establecer posiciones y prácticas de cooperación en materia de ciberseguridad.

España. Responsabilidades en el ciberespacio

Tras el análisis de las soluciones propuestas por los diferentes países y como distribuyen las responsabilidades en el ciberespacio. Se analizan las responsabilidades en España, además de la Presidencia y Vicepresidencia del Gobierno, los órganos y organismos de derecho público que, en la actualidad, tienen competencias sobre la seguridad en el ciberespacio son:

—Comisión Delegada del Gobierno para Asuntos de Inteligencia (CDGAI)

—Ministerio de la Presidencia:

- Centro Nacional de Inteligencia [13] – Centro Criptológico Nacional [14].
  - Organismo de Certificación de las TI [15]
  - CCN-CERT
- Centro Nacional de Inteligencia – Autoridad Nacional de Seguridad Delegada [16]
  - Oficina Nacional de Seguridad (ONS) [17]

—Ministerios de Asuntos Exteriores y Cooperación (MAEC).

—Ministerio de Industria, Energía y Turismo (MINETUR).

- Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI).
- Instituto Nacional de Tecnologías de la Comunicación (INTECO) [18].

—Ministerio del Interior – Secretaría de Estado de Seguridad [19]:

- Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC [20]).
- Centro Nacional de Coordinación Antiterrorista (CNCA).
- Centro de Inteligencia Crimen Organizado (CICO).
- Unidades especializadas en la lucha contra el ciberdelito y el ciberterrorismo de las FCSE.
  - Grupo de Delitos Telemáticos Guardia Civil [21]

13. Véase Centro Nacional de Inteligencia (CNI). www.cni.es

14. Véase Centro Criptológico Nacional (CCN). www.ccn.cni.es

15. Véase Organismo de Certificación. www.oc.ccn.cni.es

16. Véase Autoridad Nacional de Seguridad Delegada (ANS-D). Ver funciones en página Web CNI. www.cni.es

17. Véase Oficina Nacional de Seguridad (ONS). http://www.cni.es/es/ons/

18. Véase Instituto Nacional de Tecnologías de la Comunicación (INTECO). www.inteco.es

19. Véase Ministerio del Interior. http://www.mir.es/

20. Véase Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). http://www.cnpic-es.es/

21. Véase Grupo de Delitos telemáticos (DGT). https://www.gdt.guardiacivil.es/

- Unidad de Investigación Tecnológica del CNP [22]
- Unidad ciberterrorismo Guardia Civil

—Ministerio de Hacienda y Administraciones Públicas (MINHAP) – Secretaría Estado de Administración Pública (SEAP).

- Consejo Superior de Administración Electrónica (CSAE – AGE [23]).
- Comité Sectorial de la Administración Electrónica (CCAA)
- Otras comisiones
- Gestión de la red SARA [24]

—Ministerio de Defensa [25]:

- Estado Mayor de la Defensa (CERT-FAS).
- Secretaría de Estado de Defensa. DIGENIN [26]. Centro Operaciones de Seguridad de la Defensa (COSDEF)
- Cuartes Generales de Tierra, Armada y Aire.

—Fiscalía General del Estado – Fiscalía de Criminalidad Informática.

— CCAA. Responsabilidades en administración de sus redes y en las policías autonómicas del País Vasco, Navarra y Cataluña existen unidades que tratan este tipo de delitos.

—Equipos de Respuesta ante Incidentes nacionales, sectoriales, de las CCAA y privados. De ellos destacan:

- CCN-CERT. CERT Gubernamental
- CERT,s en el ámbito de Defensa (CERTFAS y COSDEF)
- INTECO-CERT. CERT para ciudadanos y empresas.

22. Véase Brigada de Información Tecnológica (BIT). http://www.policia.es/bit/

23. Véase Consejo Superior de Administración electrónica (CSAE). http://www.csae.map.es/

24. Sistemas de Aplicaciones y Redes para las Administraciones (SARA). Articulo 43. Ley 11/2007 de 22 junio. Acceso de los ciudadanos a los servicios públicos. Establece la interconexión de las diferentes Administraciones para intercambio de información y servicios y para la interconexión con la Unión Europea y otros Estados miembros. http://www.ctt.map.es/web/proyectos/redsara

25. Véase Ministerio de Defensa. http://www.mde.es/

26. Véase Dirección General de Infraestructuras (DIGENIN). http://www.mde.es/organizacion/organigramaMinisterio/secretariaEstado/

- IRIS-CERT. CERT para universidades y centros de investigación.
- CERT,s / SOC,s CCAA. Activos en Andalucía, Cataluña y Comunidad Valenciana. Se están desorrallando otros en Murcia, Extremadura…
- CERT,s Privados. Dan servicios de seguridad a diferentes sectores.
- Otros Centros de Operaciones de seguridad en diferentes organismos.

Equipos de respuesta ante incidentes

Actualmente, los equipos de respuesta ante incidentes se consideran los organismos con mayor capacidad técnica y con la estructura más adecuada para luchar contra el mayor espectro de ciberamenazas. El modo de actuación es muy colaborativo y sus relaciones son informales y flexibles pero guiadas por criterios de máxima eficiencia y rapidez en la actuación.

La descripción que se refleja a continuación no es exhaustiva y solo intenta proporciona una visión general de los campos de actuación de los equipos que se encuentran operando. Se relacionan a continuación:

—CCN-CERT [27]. (Organismo adscrito al CCN-CNI). Tiene responsabilidades en ciberataques sobre sistemas clasificados, sistemas de la Administración General, Autonómica y Local y, en coordinación con el CNPIC, sobre sistemas que gestionen infraestructuras críticas. Proporciona el estado de la amenaza en ciberseguridad para Presidencia de Gobierno. Este CERT es el CERT gubernamental/nacional. Tiene esta responsabilidad reflejada en el RD 3/2010 de 8 de enero que desarrolla el Esquema Nacional de Seguridad. En los artículos 36 y 37 se asigna a este CERT el papel de coordinador público estatal.

27. CCN-CERT. www.ccn-cert.cni.es

—INTECO-CERT [28] (Instituto Nacional de Tecnologías de Comunicación adscrito al Ministerio de Industria, Turismo y Comercio). Tiene responsabilidades de seguridad y respuesta ante incidentes de seguridad en los entornos de ciudadanos y pequeñas y medianas empresas (PYMES) según la definición de la comunidad sobre la que actúa este CERT. En su creación 2004 se le traspasó el CATA (Centro de Alerta Antivirus) desde Red.es, empresa pública también adscrita al Ministerio de Industria.

—CERT en comunidades autónomas (CCAA). Existen reconocidos por orden de creación el CSIRT-CV [29] de la Generalitat Valenciana, el CESICAT [30] (CERT de la Generalitat Catalana) y el ANDALUCIA-CERT. Estos organismos dependen de sus CCAA respectivas. Las responsabilidades de estos CERT,s es diferente pudiéndose referirse a los sistemas de la administración autonómica y/o local así como tener otras misiones de asistencias a empresas y ciudadanos. Se deben consultar su misión y objetivos en las páginas Web correspondientes. Se encuentran en fase de constitución diferentes CERT/SOC en Extremadura, Asturias, Murcia o Navarra.

—IRIS-CERT [31]. Organismo adscrito al Ministerio de Industria, Energía y Turismo. Tiene responsabilidades de seguridad en la red IRIS que da servicio a la comunidad universitaria y a los centros de investigación.

—Otros CERT. Existen otros CERT y centros operativos de seguridad que ofrecen servicios a otros sectores. Entre ellos destacan por su actividad los siguientes:

28. Véase INTECO-CERT. http://cert.inteco.es

29. Véase Computer Security Incident Response Team (equipo de respuesta ante incidentes de seguridad informática) de la Comunidad Valenciana CSIRT-CV. https://www.csirtcv.es/

30. Véase Centro de Seguridad de la Información de Cataluña (CESICAT). http://www.cesicat.cat/

31. Véase IRIS-CERT. http://www.rediris.es/cert/

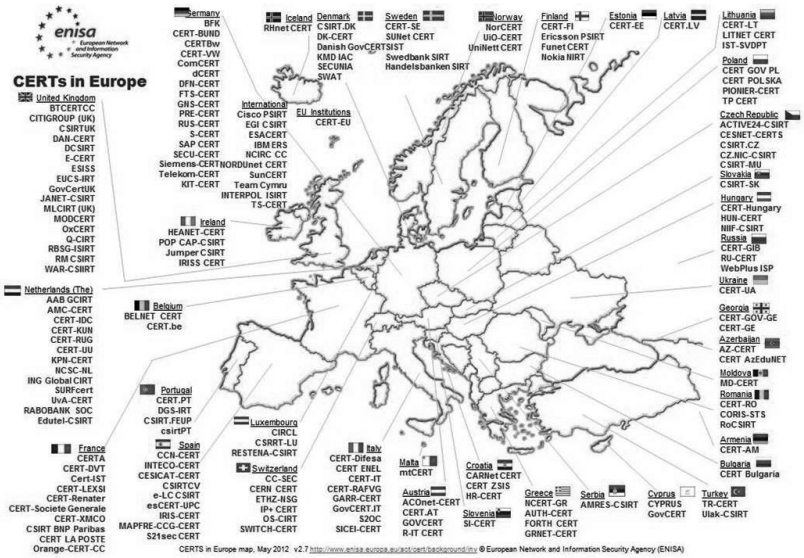
- e-La Caixa-CSIRT [32]. Respuesta ante incidentes de seguridad de este banco.
- S21Sec-CERT [33]. Este CERT proporciona servicios de gestión de incidentes para las diferentes entidades, fundamentalmente, del sector bancario).
- esCERT-UPC [34]. Decano de los CERT,s nacionales. Fundado en 1994. Proporciona servicios de CERT a la Universidad Politécnica de Cataluña.
- Hispasec [35]. Empresa de seguridad que proporciona servicios de CERT.
- MAPFRE-CCG-CERT. Proporciona servicios a esta entidad

Todos los CERT se coordinan a través del grupo de trabajo de CERT,s nacionales (CSIRT.es) [36] y a su vez, en el foro ABUSES [37] se relacionan con los principales proveedores de servicios de Internet.

En la figura adjunta se muestran los CERT,s recogidos por ENISA [38].

32. Véase E-La Caixa-CSIRT. www.lacaixa.es
33. Véase S21Sec-CERT. www.cert.s21sec.com
34. Véase EsCERT-UPC. http://escert.upc.edu/
35. Véase Hispasec. www.hispasec.com
36. Véase CSIRT.es. www.csirt.es
37. Véase Foro abuses. http://www.abuses.es/
38. Véase European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/

Figura 2



Relaciones internacionales

En el ámbito internacional existen foros de colaboración entre los organismos responsables de ciberseguridad preferentemente entre los equipos de gestión de incidentes de seguridad de los diferentes países entre los que destacan los siguientes:

—FIRST [39]. Esta organización relaciona los CERT,s reconocidos de los diferentes países resaltando su misión y la comunidad a la que proporciona servicio. La adscripción a este foro requiere un procedimiento que culmina con una auditoria realizada por uno de los CERT,s que esponsorizan la adhesión del nuevo equipo. Los CERT,s nacionales reconocidos por orden de ingreso son Iris-CERT (1997), e-La Caixa-CERT (2005), CCN-CERT (2007), EsCERT-UPC (2007), e INTECO-CERT (2008).

39. Véase Forum for Incident Response and Security Teams (FIRST). http://www.first.org/

—TF-CSIRT [40]. Grupo de trabajo de TERENA (Trans-European Research and Education Network Association). Es el foro de CERT,s europeos. Los CERT,s nacionales reconocidos por orden de ingreso son EsCERT-UPC, Iris-CERT, CCN-CERT, INTECO-CERT, CESICAT y CSIRT-CV.

—European Government CERT [41]. Es el grupo de trabajo de CERT,s gubernamentales/nacionales europeos. La adhesión a este grupo requiere una auditoria formal sobre el mandato legal, la capacidad técnica y los procedimientos empleados por el CERT. En principio solo se admite un único equipo por país. El representante nacional es el CCN-CERT.

—NCIRC [42]. Capacidad de respuesta ante incidentes de OTAN. Es la capacidad equivalente a los equipos citados anteriormente para OTAN. Identifica al CCN-CERT como CERT nacional para la coordinación de incidentes de seguridad principalmente asociado con ataques o fugas de información sensible. El CCN-CERT participa en los ejercicios de ciberdefena organizados por este organismo conjuntamente con el Estado Mayor de la Defensa (EMAD).

—Sistema de Alerta temprana de la Unión Europea. Está operativo desde principios de 2012. Identifica a los CERT,s gubernamentales para realizar el intercambio de información y para solicitar colaboración en caso de la detección de un ataque que afecte a más de una nación.

—Directorio MERIDIAN [43]. Directorio internacional de organismos y agencias gubernamentales con responsabilidad en la protección de infraestructuras críticas. No es específico de los equipos de respuesta ante incidentes aunque en los diversos aspectos que cubre el directorio aparecen estos

40. Véase TERENA. http://www.trusted-introducer.nl/

41. Véase European Government CERT http://www.egc-group.org/

42. Véase NATO Computer Incident Response Capability (NCIRC). http://www.ncirc.nato.int/

43. Véase Internacional Critical Information Infraesructure Protection Directory. Meridian conference Issue 24. Agosto 2010. No disponible en enlace público. http://www.meridianprocess.org/

equipos. En este directorio tienen responsabilidades las siguientes organizaciones; Secretaría de Estado de Seguridad (CNPIC) del Ministerio del Interior, CNI/CCN, Secretaría de Estado de Telecomunicaciones y Sociedad de la Información (SETSI) del Ministerio de Industria Turismo y Comercio, Departamento de Seguridad Nacional (DSN) de Presidencia del Gobierno y Ministerio de Defensa.

España. Situación actual

Con el panorama citado en el apartado anterior se puede ver que las responsabilidades de seguridad en el ciberespacio esta distribuida en varios organismos tanto en la Administración General de Estado como en la autonómica.

La posibilidad de solapes y sistemas que puedan depender de diversos organismos es muy alta. Además, la respuesta eficaz a las nuevas amenazas que se tienen que afrontar hace necesaria un intercambio de información muy ágil y una coordinación muy estrecha entre los diferentes organismos con responsabilidades.

En los siguientes apartados se amplia información de la problemática asociada a los siguientes ámbitos:

—Ámbitos de actuación de CERT,s.
—Sistemas de la Administración. Esquema Nacional de Seguridad.
—Sistemas asociados a infraestructuras críticas.

No se tratan la protección de datos personales y los sistemas que manejan información clasificada.

Ámbitos de actuación en ciberseguridad

Por ámbitos la actuación de estos equipos de respuesta ante incidentes sería:

—Sistemas relacionados con Seguridad y Defensa. En este ámbito por lo establecido en le RD 421/2004 la responsabilidad recae en el CCN y la respuesta ante incidentes de seguridad en el CCN-CERT. Los sistemas aquí contemplados pertenecen fundamentalmente al Ministerio de Defensa,

Ministerio del Interior, Presidencia de Gobierno, Ministerio de Política Territorial y Administración Pública y Ministerio de Asuntos Exteriores y Cooperación. Preferentemente se trata de sistemas que manejan información clasificada. Disponen de regulación propia.

—Sistemas de las Administraciones Públicas. El RD 3/2010 por el que se regula el Esquema Nacional de Seguridad determina que las responsabilidades de actuación ante cualquier incidente contra estos sistemas se ubican en el CCN-CERT, especialmente para los sistemas recogidos en el ámbito de la ley 11/2007 de Administración electrónica. Iris-CERT da servicio a la comunidad académica.

—Ciudadano y PYME. Las actuaciones en estos ámbitos en materia de prevención y respuesta están lideradas por el Ministerio de Industria, Turismo y Energía (MINETUR). La capacidad de respuesta ante incidentes se articula a través del INTECO-CERT aunque los CERT,s de las Comunidades autonómicas también se atribuyen competencias en su demarcación territorial sobre esta comunidad.

—Operadores de Telecomunicaciones y Proveedores de Servicios. los principales operadores y proveedores disponen de centros de operación de seguridad (SOC) orientados hacia la prevención y respuesta ante incidentes de seguridad, fraudes y ataques a sus infraestructuras.

—Sectores estratégicos. Empresas / Compañías de sectores considerados estratégicos como Energía, Aeronáutico, Defensa o Financiero. Existen algunos CERT de carácter privado que dan servicio a alguno de los sectores estratégicos.

—Infraestructuras críticas. La responsabilidad sobre estos sistemas recae en el CNPIC con las salvedades expuestas en el proyecto de legislación. Estos sectores se solapan con los estratégicos. Normalmente la consideración de incidente en este ámbito está asociado a la pérdida de servicio. Se desconoce el nivel de seguridad de estos sistemas. Se deberá esperar al desarrollo de la normativa asociada a la ley y RD en el campo de las TIC para poder valorar realmente el nivel de seguridad de estas infraestructuras.

Muchos de estos ámbitos de actuación se superponen y, en la gestión de incidentes de seguridad, se detectan solapes y redundancias.

Esquema nacional de seguridad

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos establece la obligatoriedad de proporcionar los diferentes servicios de la Administración en el Ciberespacio. La ley contempla la creación de sedes electrónicas desde las que los diferentes organismos deben proporcionar el máximo de servicios en línea al ciudadano.

Asimismo establece que las Administraciones Públicas utilizarán las tecnologías de la información asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

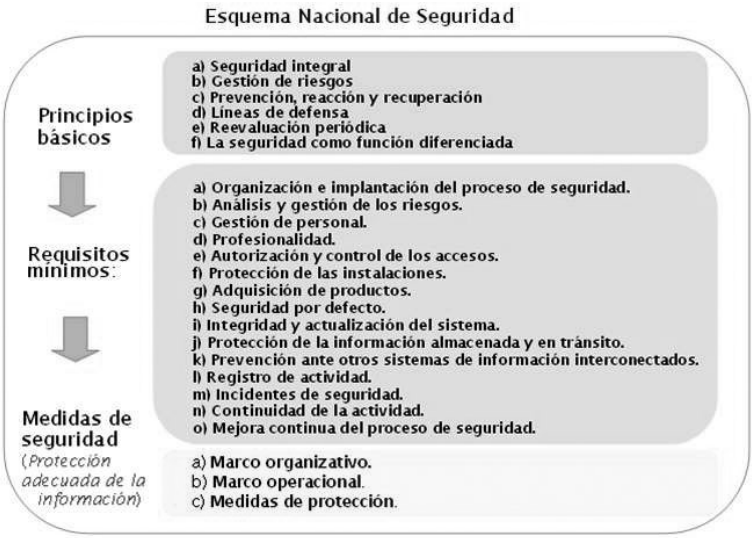
Esta ley, en su artículo 42, regula la creación de un Esquema Nacional de Seguridad que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por unos principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Este esquema ha sido publicado en el RD 3/2010 y por primera vez establece un conjunto de medidas de seguridad de obligado cumplimiento según el nivel de la información o sistema (alto, medio o bajo).

Asimismo, como aspectos interesantes del RD resaltan; la obligatoriedad de la realización de auditorias, la recomendación del empleo de productos certificados y la articulación de una capacidad de respuesta ante incidentes de seguridad para las Administraciones Públicas.

En la figura adjunta [44] se muestran estos principios básicos y requisitos mínimos.

44. Véase RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE núm. 25 (29.10.2010).

Figura 3



Asimismo, en el cuadro adjunto se muestran los diferentes servicios previstos y los organismos responsables de proporcionarlos en el ENS:

Figura 4

Se considera, por tanto, que esta norma es un conjunto homogéneo y compacto de medidas de seguridad que, una vez que se apliquen mejorarán considerablemente los niveles de seguridad de los distintos organismos de la Administración.

No obstante, el ENS adolece de algunas deficiencias fruto del consenso en su desarrollo entre la Administración General, Autonómica y Local. Así la revisión de las auditorias y la corrección de las posibles deficiencias detectadas no están supervisadas por ningún organismo que vele porque todas las AAPP mantengan el mismo nivel de seguridad en sus sistemas.

Además, aunque para sistemas de nivel alto se establece en las medidas de protección asociadas con la monitorización de sistemas, en el Real Decreto esta actividad no esta contemplada con la importancia que sería necesaria para hacer frente a las amenazas actuales.

De todas formas, el esquema en su artículo 29 establece que el CCN en colaboración con el MINHAP elaborará y difundirá guías de seguridad que desarrollen éste. Se espera que estas guías aclaren y subsanen las posibles deficiencias del mismo. En la tabla adjunta se muestra las guías previstas hasta el momento en la serie CCN-STIC 800 (en blanco las publicadas).

Figura 5

800 Esquema Nacional de Seguridad ens	800	Glosario de términos y abreviaturas del ENS	Mar-11
	801	Responsabilidades y Funciones en el ENS	Feb-11
	802	Auditoría del Esquema Nacional de Seguridad	Jun-10
	803	Valoración de Sistemas en el ENS	Ene-11
	804	Medidas de Implantación del ENS (BORRADOR)	Jul-10
	805	Política de Seguridad de la Información	Sep-11
	806	Plan de Adecuación del ENS	Ene-11
	807	Criptología de Empleo en el ENS	Sep-11
	808	Verificación del Cumplimiento de las Medidas en el ENS (BORRADOR)	Oct-10
	809	Declaración de conformidad del ENS	Jul-10
	810	Guía de Creación de CERT,s	Sep-11
	811	Interconexión en el ENS	Sep-11
	812	Seguridad en Servicios Web en el ENS	Oct-11
	813	Componentes Certificados en el ENS	Feb-12
	814	Seguridad en Servicio de Correo en el ENS (BORRADOR)	Ago-11
	815	Indicadores y Métricas en el ENS	Dic-11
	816	Seguridad en Redes Inalámbricas en el ENS	
	817	Gestión de Incidentes de Seguridad en el ENS	Ago-12
	818	Herramientas de seguridad en el ENS	
	819	Guía de contratos en el marco del ENS	
	820	Guía de protección contra Denegación de Servicio	
	821	Ejemplos de Normas de Seguridad	
	822	Ejemplos de Procedimientos de Seguridad	
	823	Requisitos de seguridad en entornos CLOUD	
	824	Informe del estado de seguridad	

Deficiencias detectadas

Se destacan las siguientes deficiencias más significativas:

1. Existencia de duplicidades y sistemas que pueden llegar a depender de diversos organismos. Los procedimientos son diferentes y los canales de intercambio de información más difíciles de implementar.
2. Ausencia de un centro coordinador en ciberseguridad que integre a todos los actores y permita al gobierno conocer la situación nacional en este campo.
3. Insuficiencia de recursos humanos, técnicos y económicos, que se encuentran disgregados en gran número de organismos, lo que dificulta satisfacer las misiones encomendadas.
4. Escaso despliegue de mecanismos de defensa en las AA.PP., lo que dificulta la adecuada respuesta ante ataques complejos. A esto hay que añadir una insuficiente gestión de infraestructuras comunes, que dispersa recursos y provoca el retraso en la aplicación del Esquema Nacional de Seguridad, como marco de referencia de buenas prácticas.
5. Reducida comunicación entre organismos del sector público y privado. Ausencia de procedimientos y sistemas que permitan un intercambio seguro de información útil y oportuna que permita la implicación del sector privado en la ciberseguridad en forma de capacidades e intercambio de información.
6. Necesidad de una capacidad técnica que en materia de ciberseguridad que posibilite la mejor aplicación de la normativa reguladora de Protección de Infraestructuras Críticas para alcanzar un conjunto integrado de medidas de aplicación a los sectores afectados.
7. Escasez de recursos destinados a las capacidades de prevención y respuesta a las actividades del terrorismo y la delincuencia en el ciberespacio.
8. Escasa actividad de desarrollo de productos nacionales con seguridad verificada. Los esfuerzos y las aproximaciones se están desarrollando en la actualidad de manera disjunta.

9. Marco normativo nacional e internacional insuficiente que no permite gestionar adecuadamente el cibercrimen.
10. Falta de concienciación de AAPP, empresas y ciudadanos sobre las ciberamenazas y las medidas para mitigarlas.

Finalmente, la respuesta eficaz a las nuevas amenazas a las que hay que hacer frente hace necesario un intercambio de información muy ágil y una adecuada coordinación entre los diferentes organismos corresponsables de la ciberseguridad, intercambio y coordinación que, con el modelo actual, resulta muy difícil de conseguir.

Estrategia española de ciberseguridad

Para resolver los solapes y deficiencias comentadas nace la Estrategia Española de Ciberseguridad (EECS) que intenta tratar de forma completa el problema y que trata de alcanzar una visión de conjunto sobre el mismo, estableciendo estructuras que aseguren la coordinación de las iniciativas de cada uno de los organismos con responsabilidades en este ámbito y promoviendo la adopción de unas líneas estratégicas de acción.

Objetivos

La Estrategia Nacional de Ciberdefensa persigue conseguir un ciberespacio más seguro a través de los siguientes objetivos:

—Lograr que España haga un uso seguro de las Redes y Sistemas de Información, fortaleciendo las capacidades de prevención, detección y respuesta a los ciberataques.
—Garantizar que los Sistemas de Información y Comunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de seguridad y resiliencia [45].
—Impulsar la seguridad y resiliencia de las Redes y los Sistemas de Información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular.

45. Resiliencia= capacidad para mantener unos niveles mínimos de servicio y recuperarse con rapidez tras un incidente.

—Potenciar las capacidades de prevención y respuesta frente a las actividades del terrorismo y la delincuencia en el ciberespacio.
—Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.
—Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad anteriores.

Líneas estratégicas de acción

Para conseguir estos objetivos se plantean algunas líneas estratégicas que se deben considerar y dotar presupuestariamente:

Línea de acción de Acción	Contenido
1. Capacidad de prevención, detección y respuesta ante las ciberamenazas	Incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa, y otros sistemas de interés nacional.
2. Seguridad de los Sistemas de Información de las AA.PP.	Implsar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3. Seguridad de las Redes y los Sistemas de Información que soportan las Infraestructuras Críticas.	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
4. Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
5. Seguridad y resiliencia en el sector privado.	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.

Conclusiones

Los ciudadanos de España, sus Administraciones Públicas y sus empresas han incorporado masivamente el uso de Internet y las nuevas tecnologías a su quehacer cotidiano, personal o profesional, participando, al tiempo, tanto de las enormes oportunidades que comportan como de sus innegables riesgos.

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Además no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas

Las ciberamenazas se incrementan incesantemente, desde multitud de orígenes y con motivaciones diferentes, afectando transversalmente al sector público, al privado y a los propios ciudadanos. Los ciberdelincuentes, el crimen organizado, los grupos terroristas, el hacktivismo antisocial o, incluso, los propios estados, son capaces de explotar las vulnerabilidades tecnológicas con el objeto de recabar información, sustraer activos de gran valor y amenazar servicios básicos para el normal funcionamiento de nuestro país.

Todas las naciones de nuestro entorno están desarrollando iniciativas para intentar controlar las amenazas que vienen del ciberespacio. La mayoría de ellas esta apostando por estrategias similares a la propuesta en este documento.

En España las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos que abordan el problema de forma parcial.

Es necesario por tanto impulsar actuaciones en este sentido fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante este tipo de amenazas. La dotación presupuestaria se considera crítica si se quieren llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la amenaza.

Por ello, la estrategia propone que se establezca un programa que afecte a todo la nación para alcanzar los objetivos estratégicos planteados incrementando los fondos que desarrollen nuevas tecnologías para proteger las redes nacionales e incrementando

la formación en perfiles críticos para esta actividad y fomentando el trabajo coordinado entre el sector público, la industria, los ciudadanos y los aliados internacionales.

Bibliografía

[Ref.-1] CCN-CERT IA-04/12 Ciberamenazas 2011 y Tendencias 2012
Febrero de 2012
Informe de amenazas del CCN-CERT
www.ccn-cert-cni.es (parte privada del portal)

[Ref.-2] [Cyber Threats and Trends
18 de diciembre de 2012
An iDefense® Topical Research Paper
The VeriSign® iDefense® Intelligence Operations Team

[Ref.-3] 16 th Annual
CSI Computer Crime and Security Survey
Diciembre de 2011

[Ref.-4] A human capital crisis in cybersecurity.
Technical Proficiency Matters.
July 2010. Center for Strategic & International Studies.
www.csis.org

[Ref.-5] Internacional Critical Information Infraestructure Protection Directory. Meridian conference
Issue 27. Spain (Pág. 110)
Julio 2012

[Ref.-6] Oscar Pastor, Jose Antonio Pérez, Daniel Arnaiz, Pedro Taboso.
Cuadernos Cátedra ISDEFE-UPM
Seguridad Nacional y Ciberdefensa
Octubre de 2009

[Ref.-7] ENISA Country Reports
European Network and Information Security Agency (ENISA)
Junio 2012
http://www.enisa.europa.eu/

[Ref.-8] Committee from the Comission to de European Parliament, the Council and the Committee of the Regions. Toward a general policy on the fight against cyber crime 22 de mayo de 2007

[Ref.-9] José María Molina Mateos
Aspectos jurídicos de la protección criptológica de la información y las comunicaciones"
Universidad Complutense, Madrid 1999.

Legislación

[Ref.-10] RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
BOE núm. 25 de 29 de enero de 2010.

[Ref.-11] LEY 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
BOE núm. 109 de 7 de mayo de 2002

[Ref.-12] REAL DECRETO 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
BOE núm. 68 de 19 de marzo de 2004

[Ref.-13] LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
BOE núm. 150 23 de junio de 2007

[Ref.-14] ORDEN PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
BOE núm. 230 25 de septiembre de 2007

[Ref.-15] Ley 08/2011 de 28 de abril por la que se establecen medidas para la protección de las infraestructuras críticas.
RD 704/2011 de 20 de mayo, por el que aprueba el Reglamento de medidas para la protección de las infraestructuras críticas
www.cnpic-es.es
Fecha de consulta 11 de septiembre de 2012

[Ref.-16] Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

[Ref.-17] Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
BOE núm. 25 de 29 de enero de 2010.
Reino Unido

[Ref.-18] Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space. June 2009
Cabinet Office
www.cabinetoffice.gov.uk

[Ref.-19] Rex Hughes and David Livingstone
Cyberspace and the National Security of the United Kingdom
Paul Cornish, Chatham House, March 2009
Estados Unidos

[Ref.-20] The National Strategy to Secure Cyberspace.
White House. Washington
February 2003
http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
Fecha de consulta 07 de octubre de 2012

[Ref.-21] Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure
29 de mayo de 2009 www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
Fecha de consulta 07 de octubre de 2010

[Ref.-22] The Comprehensive National Cybersecurity Initiative
Año 2010
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
Fecha de consulta 07 de octubre de 2012
Canadá

[Ref.-23] Canada´s Cyber Security Strategy. For a stronger and more prosperous Canada. 2010
http://www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.aspx
Fecha de consulta 07 de octubre de 2012
Estonia

[Ref.-24] Cyber Security Strategy. Cyber Security Strategy Committee
Ministry of Defence. ESTONIA
Tallinn 2008
http://www.mod.gov.ee/en/national-defense-and-society
Fecha de consulta: 09 de octubre de 2012
Francia

[Ref.-25] Défense et Sécurité nationale. LE LIVRE BLANC
Editorial Odile Jacob/ La Documentation Francaise
Junio 2008
http://www.livreblancdefenseetsecurite.gouv.fr/
Fecha de consulta: 10 de octubre de 2012

[Ref.-26] Plan ded Reforcement de la Securite des Systemes d´Information de Létat
Marzo 2004
www.ssi.gouv.fr
Fecha de consulta: 10 de octubre de 2012

[Ref.-27] L'Agence nationale de la sécurité des systèmes d'information (ANSSI) decreto n° 2009-834 de 7 de julio de 2009 (Journal officiel du 8 juillet 2009).
www.ssi.gouv.fr
Fecha de consulta: 10 de octubre de 2012
Alemania

[Ref.-28] Act to Strengthen the Security of Federal Information Technology of 14 August 2009
Act on the Federal Office for Information Security (BSI Act – BSIG).
www.bsi.bund.de/
Fecha de consulta: 01 de octubre de 2010

[Ref.-29] Improving IT Security
BSI Annual Report 2008/2009
Federal Office for Information Security BSI

www.bsi.bund.de
Fecha de consulta: 01de octubre de 2010

[Ref.-30] National Plan for Information Infrastructure Protection
Octubre 2005
www.bmi.bund.de
Fecha de consulta: 01de octubre de 2010
Australia

[Ref.-31] Cyber Security Strategy
Attorney General's Department,
23 de noviembre de 2009
http://www.ag.gov.au/cybersecurity
Fecha de consulta 07 de octubre de 2010

[Ref.-32] Protecting Yourself Online. What Everyone Needs to Know
Australia 2010
www.staysmartonline.gov.au
Fecha de consulta 07 de octubre de 2010

[Ref.-33] E-SECURITY REVIEW 2008
DISCUSSION PAPER FOR PUBLIC CONSULTATION
http://www.ag.gov.au/agd/agd.nsf
Fecha de consulta 07 de octubre de 2010

[Ref.-34] Security of Infrastructure Control Systems for Water and Transport
VICTORIAN GOVERNMENT PRINTER
October 2010
www.audit.vic.gov.au
Fecha de consulta 05 de octubre de 2010

OTROS TITULOS DE LA COLECCIÓN BIBLIOTECA CONDE DE TENDILLA

Guerra, Ejército y Sociedad en el nacimiento de la España contemporánea
Beatriz Freyro de Lara (Coord.)

Constitución y Fuerza Militar (1808-1978)
Ramón Gómez Martínez

El conde de Tendilla. Primer capitán general de Granada
José Smolka Clares

Manual militar para periodistas
José Luis Serrano Ramírez

Militares y Oenegés. Reflexiones sobre una relación a veces tormentosa
Javier Ruiz Arévalo

Defensa y Globalización
Carlos de Cueto Noguera, Adolfo Calatrava (Coords.)

La nueva política de seguridad de la Unión Europea
Javier Roldán Barbero (Coord.)

Género, conflictos armados y seguridad. La asesoría de género en operaciones
Margarita Robles Carrillo (Coord.)

La conciencia intercultural (Cross-cultural awareness) en la resolución de crisis y conflictos
Concepción Pérez Villalobos, Humberto Trujillo Mendoza (Coords.)

Bioseguridad, Derecho y Defensa
M.ª Ángeles Cuadrado Ruiz y Antonio Peña Freire (Eds.)

Derecho militar español
M.ª Concepción Pérez Villalobos (Coord.)

Elementos de cultura y transculturalidad para usos militares y civiles
José Antonio González Alcantud (Dir.)

Culturas cruzadas en conflicto
Marién Durán Cenit, Antonio Ávalos Méndez

La dimensión psicosocial, política y jurídica de la consciencia transcultural: el caso de Afganistán
Humberto M. Trujillo Mendoza (Coord.)

Radicalización islamista y terrorismo. Claves psicosociales
Manuel Moyano y Humberto M. Trujillo Mendoza

Ciberseguridad global. Oportunidades y compromisos del uso del ciberespacio
Antonio Segura Serrano, Fernando Gordo García (Coords.)