Tema central

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563

Urvio, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 80-93
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad

Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity

Vicente Pons Gamón[1]

Fecha de recepción: 7 de febrero de 2017
Fecha de aceptación: 26 de abril de 2017

Resumen

El artículo tiene como objetivo analizar la visión que tienen diversos autores sobre la aparición del ciberdelito en materia de terrorismo (ciberterrorismo) y la respuesta de las naciones en defensa cibernética. En primer lugar estudiamos el nacimiento de un nuevo espacio delictivo el "ciberespacio" y todas sus amenazas, en una segunda parte vemos la reacción que este fenómeno ha provocado en las naciones y organizaciones internacionales en dirección a determinar y estudiar todos estos delitos, sus causas, métodos y reacciones, para poder combatirlos desde el aspecto legal (legislación española, europea e internacional) y a partir de aquí finalizar mostrando la visión estratégica de defensa de los estados, estudiando como ejemplos las líneas de actuación que utiliza España y Europa para contrarrestar su efecto destructivo en la sociedad actual.

Palabras clave: Ciberespacio; Cibercrimen; Ciberdelincuencia; Ciberdelito; ciberterrorismo; ciberataque; ciberdefensa.

Abstract

This article aims to analyze the view of different authors about emergence of cybercrime in the terrorism area (cyberterrorism) and the nations cyber-defense response. In a first time we study the birth of a new criminal space "cyberspace" and all its threats, in a second part we see the reaction that this phenomenon has provoked to nations and international organizations in order to determine and study all these crimes, methods and reactions, so as to be able to combat them from the view legal point (Spanish, European and internacional legislation) then finish, showing the strategic vision of states defense, studying as examples the lines of action used by Spain and Europe to counteract its destructive effect on today's society.

Keywords: Cyberspace; Cybercrime; Cyberdelinquency; cyberterrorism; cyberattack; cyberdefense.

1 Licenciado por la Universidad de Valencia y Posgrado en la Facultad de Ciencias Económicas y Empresariales Universidad Nacional de educación a distancia (UNED). Máster en Seguridad y Doctorando en Derecho y Ciencias Sociales por la UNED (España). Correo: vp@infurma.es

Introducción

La aparición de internet y los sistemas informáticos supuso un antes y un después en el modo que las personas acceden a los sistemas de información, donde cada acción se encuentra reflejada, pues "la red es un nuevo espacio donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día" (Alonso García 2015, 18). También se comenzaron a evidenciar los comportamientos delictivos en torno a estos nuevos paradigmas y herramientas cibernéticas. Durante estos periodos de crecimiento de las redes informáticas, los llamados ciberdelincuentes avanzaron a pasos agigantados desarrollando técnicas y métodos para vulnerar unos sistemas de seguridad, aún inmaduros, tomando ventaja sobre las autoridades y su escasa preparación para abordar este nuevo problema.

Esta investigación se centra en las acciones delictivas en el ciberespacio, que hoy por hoy, preocupan a las naciones y a sus cuerpos de seguridad, más aún si provienen de grupos u organizaciones terroristas. Partimos, como idea clave, del nuevo concepto de ciberespacio, y veremos, entre otras, las definiciones de ciberdelincuencia y ciberterrorismo, las ventajas y las técnicas de los ciberataques. Posteriormente, se tratará de conocer la reacción y líneas de acción de naciones y organizaciones, con especial referencia a España.

Nacimiento de un nuevo espacio delictivo: el "ciberespacio"

Históricamente, comenzamos a hablar del nacimiento del internet en 1969. Desde su surgimiento, la conocemos como el conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP (trasmisión control protocol/internet protocol), que garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial. Es interesante recordar que "la red de redes nació de la idea y de la necesidad de establecer múltiples canales de comunicación entre ordenadores" (Chicharro Lázaro 2009, 4), y que "el advenimiento de internet y su expansión han demostrado ser una de las revoluciones tecnológicas más importantes de la historia contemporánea" (Carlini 2016, 3).

Este fenómeno es tan revolucionario que en unos pocos años se produce un enorme incremento en el número de usuarios de internet, "en 1993 se estimaba que había 14 millones y en julio de 2014 rondaban los 2900 millones" (Carlini 2016, 3). En la actualidad, todos los ciudadanos y las sociedades que conforman, tienen una dependencia casi total de los sistemas informáticos para todos los procesos económicos y sociales, que además están íntimamente relacionados. Este rápido y acelerado crecimiento de las tecnologías de información abrió espacios para el delito, poniendo un arma de gran calibre en manos de los delincuentes y terroristas.

Así, desde esta misma óptica, siguiendo a Curtis (2011), podemos describir al espacio cibernético, o ciberespacio, como un dominio artificial construido por el hombre, diferenciado de los otros cuatros dominios de guerra (tierra, aire, mar y espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa. Además, el ciberespacio no está aislado sino profundamente vinculado y apoyado por medios físicos, por ejemplo las redes eléctricas. Si se ataca a esta interconexión puede tener repercusiones graves sobre

las estrategias de seguridad, nacionales e internacionales.

A partir del desarrollo acelerado de la internet, también emerge el lado oscuro y surgen nuevos términos como *cibercrimen, ciberdelito o ciberdelincuencia*, que describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio y que tienen cuatro características específicas: "se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas" (Subijana Zunzunegui 2008, 171).

Centrándonos en el origen y aparición de los ciberataques, y posteriormente, ciberterrorismo, Ponce (2012) considera que "el advenimiento de la Web 2.0 revoluciona el concepto de red", donde todos compartimos información que es actualizada constantemente; y también menciona que "la Web 2.0 se ha llamado en muchas ocasiones a la Web social y los medios de comunicación que ofrece, también han incorporado este adjetivo, denominándose Medios Sociales o Social Media".

Como indica Urueña Centeno (2015) "el ataque se puede realizar desde cualquier parte del mundo, lo que ofrece al ciberdelincuente varias ventajas". Si analizamos estas ventajas podemos indicar lo siguiente: el ciberatacante se siente seguro, ya que no se expone físicamente a su víctima ni mucho menos a la posible intervención de las fuerzas de seguridad, dado que su acción delictiva se realiza *a distancia*; sensación de cómoda impunidad, al saber que hay lagunas legislativas a nivel internacional, por lo que muchos de los delitos cometidos no *se castigan*. Además, el delincuente aprovecha el anonimato de sus ciberacciones al ser complicado identificar al atacante; cualquier usuario que tenga un equipo informático y conexión a internet, con unos conocimientos técnicos que están al alcance de cualquiera y con una inversión económica no elevada, puede ejecutar un ciberataque; cualquier ciberataque conlleva un efecto de vulnerabilidad y falta de protección individual; y por último estos ataques sacuden la opinión pública y tiene gran difusión en los medios digitales de todo el mundo.

Entre los delitos tipificados como ciberdelincuencia encontramos: *el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos*. Con las últimas modificaciones legislativas, se han introducido otros delitos que emplean las tecnologías de la información y la comunicación, tales como el acoso electrónico contra la libertad de personas, el descubrimiento y revelación de secretos, la interferencia ilegal de información o datos, los delitos contra la propiedad intelectual y los abusos con fines sexuales a través de internet u otros medios de telecomunicación a menores. En el gráfico 1 se resume en series temporales, datos entre los años 2011 a 2015, que corresponden a la actividad registrada por las Fuerzas y Cuerpos de Seguridad del Estado Español (Guardia Civil y Policía Nacional) y la Policía Foral de Navarra. También se incluyen datos de los cuerpos de policía local que facilitaron estadísticas al Sistema Estadístico de Criminalidad durante el año 2015. Como se puede apreciar la tendencia al alza es continua, produciéndose un incremento de más de 10.000 delitos en 2015 con respecto a 2014.

Gráfico 1. Cibercriminalidad y principales tipologías penales cometidas con las nuevas tecnologías

Grupos delictivos	2011	2012	2013	2014	2015
Acceso e interceptación ilícita	1.492	1.701	1.805	1.851	2.386
Interferencia en los datos y en el sistema	228	298	359	440	900
Falsificación informática	1.860	1.625	1.608	1.874	2.361
Fraude informático	21.075	27.231	26.664	32.842	40.864
Delitos sexuales	755	715	768	974	1.233
Contra la propiedad industrial/intelectual	222	144	172	183	167
Contra el honor	1.941	1.891	1.963	2.212	2.131
Amenazas y coacciones	9.839	9.207	9.064	9.559	10.112
Total	**37.412**	**42.812**	**42.403**	**49.935**	**60.154**

Fuente: Ministerio del Interior, España (2016).

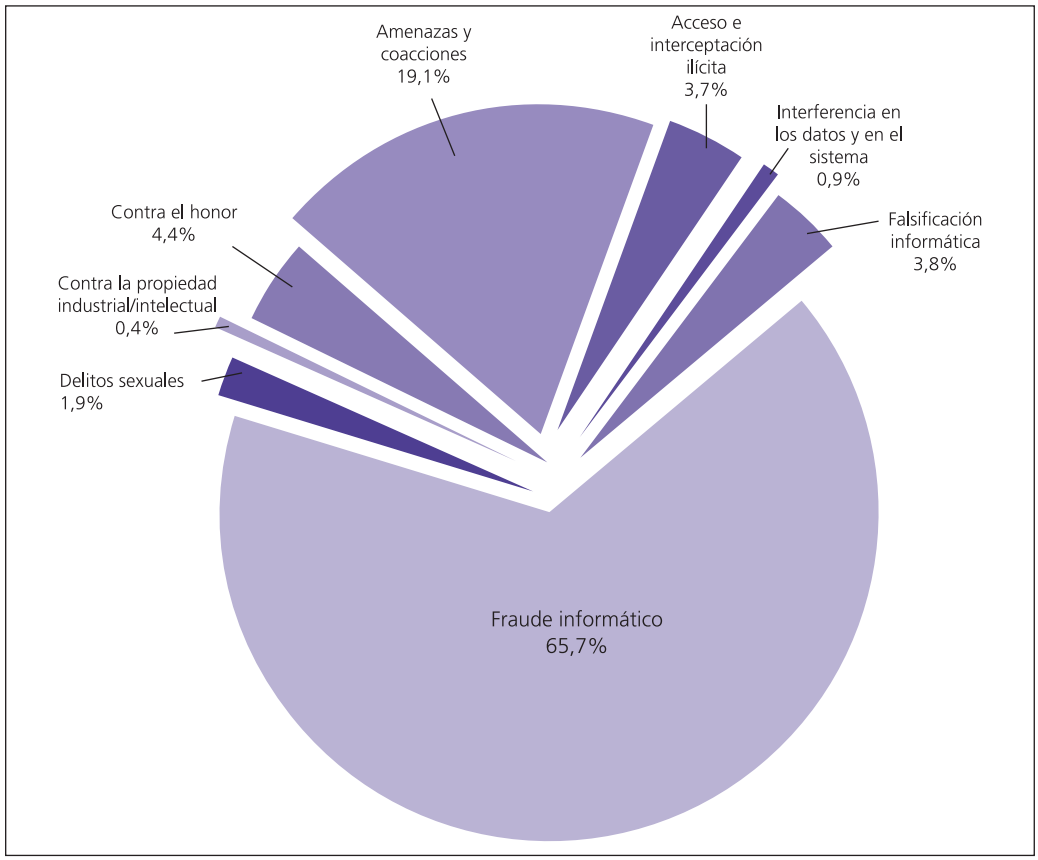
En el gráfico 2 se observa la distribución porcentual de los ciberdelitos en 2015, de los cuales podemos indicar que el fraude informático (65,7%) es el principal delito cometido en la actualidad, seguido de las amenazas y coacciones (19,1%) y la falsificación informática (3,8%).

Centrándonos ahora en los instrumentos o técnicas que se utilizan en los ciberataques de mayor o menor intensidad y siguiendo a Urueña Centeno (2015, 4-5) y el último informe de la Agencia europea para la Seguridad de las Redes y de la Información (ENISA), hacemos referencia a las quince amenazas más relevantes: *Malware*; ataques basados en el uso de la web; ataques basados en aplicaciones web; denegación de servicio; *botnets*; *phishing*; correo basura (*spam*); *ransomware*; amenaza interna; daños físicos, robos o pérdidas; kit de explotación de vulnerabilidades; violación de datos; robo de identidad; fuga de información; y ciberespionaje.

El *malware* es el nombre que agrupa a distintos *software* maliciosos como virus, gusanos o caballos de Troya, que crecen rápidamente y afectan a los contenidos de los sistemas informáticos al que accede. En relación con los ataques basados en el uso de la web, hay que indicar que existe gran variedad, como por ejemplo, las web que visita el usuario y compromete a su equipo, abren puertas traseras y vulneran su navegador. También se usan ataques a través de una aplicación web, quedando expuestos o vulnerables sectores importantes como la administración pública.

Los ataques por denegación de servicio (DDoS, *Denial of service*) hacen que sea imposible el acceso a los propios recursos y servicios de una organización o empresa y posteriormente solicitan un rescate para detener los ataques. El "*bot*" es otro programa malicioso utilizado para tomar el control de un equipo informático, sin que sea detectado fácilmente. El *phishing* es el término informático que se utiliza cuando el atacante intenta suplantar la identidad de cualquier víctima para adquirir su información confidencial. El conocido de forma universal como spam o correo basura, centra su acción en el envío de correos a un gran número de usuarios perjudicando al receptor.

Gráfico 2. Porcentaje de tipos penales relacionados con la cibercriminalidad en España (2015)



Fuente: Ministerio del Interior, España (2016).

El *ransomware* es otro software malicioso que infecta y le da al atacante la posibilidad de bloquear su equipo informático y controlar sus datos. En relación con la amenaza interna hay que indicar que se trata de una persona o agente, normalmente empleado o funcionario de una institución que tiene acceso a los programas informáticos de la organización para causar un incidente grave de seguridad. El robo o pérdida de material sensible, también se considera como una amenaza que afecta a la fuga de datos y robos de identidad. Si se tiene un conocimiento y habilidades especiales, se puede desarrollar un kit de explotación de vulnerabilidades de seguridad para tener una posición dominante sobre los competidores tanto económicos como institucionales, esas habilidades pueden proporcionar una brecha o violación de datos de carácter confidencial, robar la identidad, violar los datos correspondientes a registros personales, o realizar operaciones de espionaje cibernético a gran escala.

Cabe esperar, por su grado de importancia, que las autoridades mundiales encargadas de defender y aplicar leyes enciendan motores, para evitar y perseguir este tipo de delitos.

Analizando los alcances e implicaciones de los medios informáticos en acciones delictivas, podemos hacer un recorrido por la definición de *ciberterrorismo*, partiendo que "delito informático o ciberdelincuencia, es toda aquella acción ilegal que se da por las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet" (Urueña Centeno 2015, 2). Muchos de esos delitos, aún no están tipificados como tales en la ley y se definen actualmente como abusos informáticos. La forma más destructiva de ciberdelincuencia es el ciberterrorismo donde convergen el ciberespacio y el terrorismo, por lo que esta forma de acción utiliza las tecnologías de la información para conseguir sus fines, intimidando, atemorizando y causando daño a sus víctimas. Actualmente, para la preparación y ejecución de casi la totalidad de acciones terroristas están apoyadas cibernéticamente o utilizan en algún momento medios cibernéticos en su realización bien para comunicación o acción.

Chicharro Lázaro (2013) define ciberterrorismo como "el uso de las nuevas tecnologías con fines terroristas". Los terroristas pueden usar las herramientas informáticas como objeto de ocasionar daños, lanzando ataques de cualquier tipo contra equipos informáticos, redes o información recogida en ellos. También, pueden ejecutar atentados a través del empleo de cualquier acción de las contempladas anteriormente contra los sistemas individuales y de redes, causando daños físicos, y por último, pueden servirse de internet para su propaganda, incitación, amenazas, hacer proselitismo, financiar sus ataques y reclutar a nuevos simpatizantes que con un poco de entrenamiento y consignas estarán en condiciones de servir a la causa terrorista.

Si nos referimos al uso que los terroristas hacen en este nuevo ciberespacio, hay que indicar, tal y como refiere Conway (2006, 7), que internet tiene la capacidad de conectar no solo a miembros de las mismas organizaciones terroristas, sino también a miembros de diferentes grupos. Así por ejemplo, existen cientos de sitios "yihadistas" en todo el mundo que expresan su apoyo al terrorismo, y en estas web y foros conexos que permiten a terroristas en lugares tan lejanos como Chechenia, Palestina, Indonesia, Afganistán, Turquía, Irak, Malasia, Filipinas y Líbano intercambiar no solo ideas y sugerencias, sino también información práctica sobre cómo construir bombas, establecer células terroristas y, en última instancia, perpetrar ataques.

El Consejo de Europa define el ciberterrorismo como al "terrorismo que utiliza las tecnologías de la información para poder intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos" (Subijana Zunzunegui 2008). La ciberdelincuencia y el ciberterrorismo buscan desestabilizar las estructuras sociales establecidas. España fue el tercer país, tras Estados Unidos y Reino Unido, que mayor número de ataques cibernéticos sufrió en 2014. Según declaraciones del ministro de Asuntos Exteriores, existieron más de 70.000 ciberincidentes de los que no detalló la gravedad (González 2015). Los crímenes del ciberterrorismo, cuando tienen intención de causar pánico colectivo, una alarma social generalizada, responden a una motivación ideológica determinada, conllevan implicaciones más graves que los delitos comunes para la seguridad nacional y la política de defensa.

Determinando que el origen del ciberterrorismo radica intrínsecamente en su misma raíz como *espacio cibernético*, escenario dónde se desarrollan las amenazas cibernéticas. Si tomamos como base la conceptualización emanada del Departamento de Defensa de los

Estados Unidos (2016), el ciberespacio sería "un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores". Estas nuevas ventajas son usadas por las organizaciones terroristas para el cumplimiento de sus objetivos estratégicos, el funcionamiento de cuidadosas estrategias de marketing, una adecuada utilización de redes sociales virtuales, y así conseguir recursos económicos y otros, con el fin de realizar su cruzada armamentista.

Existe un consenso alrededor de esto, y es que los ciberataques, en sus diferentes modalidades, entre las que se encuentra su máxima expresión, el ciberterrorismo, representan la mayor amenaza no solo para el individuo, sino también para la sociedad en su conjunto. Se considera que los "ciberataques son hoy en día la estrategia de guerra más poderosa" (Urueña Centeno 2015). A raíz de esto, el Consejo de Europa, en su Convenio sobre la ciberdelincuencia promulgado el 23 de noviembre de 2001 en Budapest, y ratificado por España el año 2010, engloba las actuaciones de ciberdelincuencia y tipifican las diversas actividades realizadas en el ciberespacio, dirigidas a diversos objetivos, que por su naturaleza serían constitutivos de delito. Entre estas, podemos encontrar delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (acceso ilícito, interceptación ilícita, interferencia en datos, interferencia en el sistema y abuso de dispositivos); delitos informáticos (falsificación informática o fraude informático); delitos relacionados con el contenido (pornografía infantil: producción, puesta a disposición, difusión, adquisición o posesión de la misma por medio de un sistema informático); y delitos relacionados con infracciones de propiedad intelectual y de derechos afines (Instrumento de Ratificación 2001).

Analizando las ciberamenazas terroristas, se presupone que las consecuencias más significativas de este tipo de delitos son económicas y de imagen, aunque por supuesto, no debemos quitar importancia a los relacionados con el contenido. Los ataques son cada vez más sofisticados y afectan redes informáticas que en teoría disponen de niveles de seguridad extremos, es entonces cuando a este análisis de las implicaciones de los ciberataques, el factor económico aparece con un elemento que definido como "inteligencia económica como el conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico" (Olier Arenas 2013, 9). Estas acciones se focalizan en el ámbito de economía nacional y también a menor nivel en sectores pequeños sectores empresariales, dada la globalización de los mercados que pone también en riesgo a las compañías menores.

En el mismo orden de ideas aparece otro fenómeno delictivo, *el ciberespionaje*, que afecta de manera obvia a la seguridad de la información, tiene amplia incidencia en el sector económico, debido a que "las grandes empresas multinacionales sufren igualmente el acoso de espías electrónicos, en busca de información sobre nuevos proyectos de desarrollo, en un entorno altamente globalizado y competitivo" (Ruiz Díaz 2016, 14). Una vez definido el nuevo espacio virtual donde se cometen determinados delitos, gracias a las ventajas sobre la forma tradicional que realizan los delincuentes o terroristas, y conocidos los grupos delictivos tipificados en la legisla-

ción española como ciberdelincuencia, hemos comprobado la tendencia al alza de manera continua durante los últimos años, y además, se ha tratado de determinar la definición de ciberterrorismo, por lo que podemos pasar al siguiente apartado para analizar la reacción defensiva que este fenómeno ha provocado en las naciones, para poder combatirlo desde la legalidad.

Reacción de naciones y organizaciones

Desde la aparición de los ciberataques realizados por delincuentes, por el crimen organizado o por terroristas, las naciones y organizaciones han ido reaccionando de forma progresiva para enfrentarse contra esta amenaza global. De esta forma, se han creado estrategias y sistemas de respuesta para garantizar la seguridad de sus ciudadanos y empresas. Así, se han ido modificando y adaptando la legislación de los distintos países y organizaciones. En el ámbito jurídico internacional, siguiendo el *ius ad bellum* de la Carta de las Naciones Unidas (ONU), este tipo de ataques cibernéticos de un Estado contra otro, tienen la siguiente consideración: podrían ser considerado como "uso de la fuerza" y pueden provocar un conflicto armado internacional; el Estado atacado tendría derecho a defenderse legítimamente mediante un ataque armado; de forma general el Consejo de Seguridad considera estos actos como de agresión y amenaza a la paz, por lo que podría intervenir para restablecer la paz y la seguridad internacional.

Carlini (2006, 8) indica que "para entender mejor los ataques cibernéticos como *uso de la fuerza* tendría que tenerse en consideración el instrumento, el objeto y un enfoque basado en los efectos". Igualmente el trabajo realizado por el Grupo de Expertos del Centro de Excelencia de la OTAN (Organización del Tratado del Atlántico Norte, *North Atlantic Treaty Organization NATO*) para la Ciberdefensa de Tallín, menciona que el derecho internacional vigente es de aplicación a las operaciones cibernéticas y los Estados podrán ejercer el derecho de la legítima defensa (CCDCOE 2013).

Este tipo de actos y la dificultad para su tipificación en materia jurídica ha obligado a las naciones a actualizar los conceptos de seguridad y defensa, debido a las diversas razones que han producido un incremento del riesgo.[2] Entre estas, encontramos "la diversificación de actores (o activos que son potenciales objetivos), dentro de la seguridad y la defensa (organizaciones públicas, civiles y militares, organizaciones privadas y ciudadanos)"; y la "diversificación y aumento de las amenazas (los terroristas y las organizaciones criminales, las naciones hostiles, personal descontento, catástrofes naturales y el simple ciudadano que persigue notoriedad)" (Pastor Acosta *et. al*. 2009).

Este incremento de riesgos está asociado a las vulnerabilidades de los sistemas, de acuerdo a la Escuela de Altos Estudios para la Defensa Española, que lo define como "cualquier debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas". Las vulnerabilidades no solo son características inherentes a la naturaleza de sus activos, pues también se considera una vulnerabilidad la presencia de errores de diseño, implementación, operación o administración de un sistema de información pudiendo ser explotados,

2 Riesgo: estimación del grado de exposición a que una amenaza se materialice, a través de las vulnerabilidades, sobre uno o más activos causando daños o perjuicios sobre los mismos.

y deriven en un efecto no deseado o no esperado que comprometa la directiva de seguridad del sistema (Ministerio de Defensa 2014).

Para contrarrestar los riesgos y vulnerabilidades, los Estados toman las medidas necesarias, pero estos no pueden tomar acciones fuera de pactos internacionales, si nos atenemos al artículo 2 (párrafo 4) de la Carta de la ONU sobre el "uso de la fuerza". Aun así, los Estados afectados deben responder mediante su Derecho Penal nacional antes de tomar en consideración una intervención del Consejo de Seguridad, para preservar la paz y la seguridad. Además, hay que tipificar los delitos graves suficientemente para que se puedan enjuiciar y sancionar estas conductas terroristas descritas, de forma que quede debidamente reflejada la gravedad del delito. Las acciones terroristas constituyen el máximo exponente de nuevas amenazas que el terrorismo internacional plantea a las sociedades abiertas, que pretenden poner en riesgo los pilares en los que se sustenta el Estado de Derecho y el marco de convivencia de las democracias del mundo (Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo).

El terrorismo internacional, concretamente el yihadista, se caracteriza ser el que más emplea la red para la divulgación de sus ideas y sus métodos de ataques, así incorporan nuevas formas de agresión, sobre todo orientadas a la captación, adiestramiento o adoctrinamiento en el odio, que no tendrán reparaos en emplear de manera cruel contra sus enemigos. Los Estados deben, combatir esta amenaza con todos sus instrumentos legales a su alcance.

Si particularizamos en el caso español, las herramientas legales son de diversa índole, su legislación relacionada con la Seguridad Nacional y Ciberdefensa, se encuentra recogida en la Ley 36/2015, de 28 de septiembre de Seguridad Nacional, en la Estrategia de Seguridad Nacional de 2013, la Estrategia de Ciberseguridad Nacional de 2013 (Consejo de Seguridad Nacional 2013), y concretamente, en un conjunto de artículos del Código Penal español y Leyes tratan directa o indirectamente el tema del terrorismo: Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.

Además, el Estado español modificó sus estructuras, en varios ministerios, para dar respuesta a las ciberamenazas y ciberterrorismo, por ejemplo se creó el Instituto Nacional de Ciberseguridad (INCIBE)[3], la Oficina Nacional de Seguridad (ONS), el Centro Criptológico Nacional (CCN), el Mando Conjunto de Ciberdefensa, el Centro Nacional para la protección de las Infraestructuras Críticas (CNPIC), o unidades especializadas dentro de los cuerpos de seguridad como el Grupo de Delitos Telemáticos y Grupo de Ciberterrorismo de la Guardia Civil.

En el seno del INCIBE opera el centro de respuesta a incidentes de ciberseguridad (*ComputerEmergency Response Team* CERT) de Seguridad e Industria (CERTSI)[4], que por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015 es el CERT Nacio-

3 El INCIBE es un organismo que trabaja en la prevención y protección frente a incidentes de seguridad de la información que colabora con iniciativas de colaboración público-privadas para mejorar los niveles de ciberseguridad en España.

4 El CERTSI es un centro de respuestas a incidentes derivados de las tecnologías de la información de las infraestructuras críticas ubicadas en España y actúa como la primera línea estratégica de acción que incrementa la capacidas de prevención, detección, investigación y respuesta ante las ciberamenazas.

nal competente en la prevención, mitigación y respuesta ante incidentes de ciberseguridad. El CERTSI ofrece capacidad tecnológica y de coordinación, de forma continuada 24 horas al día, 7 días a la semana, en tres ámbitos diferenciados: ciudadanos y empresas; Instituciones afiliadas a la RedIRIS; y operadores estratégicos y de infraestructuras críticas.

La experiencia de lucha contra el terrorismo en España permite contar con una legislación penal eficaz que ya dio respuesta al terrorismo protagonizado por extintas bandas armadas como ETA (*Euskadi Ta Askatasuna*) o el GRAPO (Grupo de Resistencia Antifascista Primero de Octubre). El eje del tratamiento penal del terrorismo era la definición de la organización o grupo terrorista y la tipificación de aquellas conductas que cometían quienes se integraban en ellas o prestaban su colaboración. El Código Penal español no debe perder esa perspectiva de tipificación de las conductas articuladas en torno a organizaciones o grupos terroristas.

Estas nuevas amenazas exigen la actualización de la normativa para dar cabida al fenómeno del terrorismo individual y a conductas que constituyen la principal preocupación de la comunidad internacional, en línea con la Resolución 2178 del Consejo de Seguridad de Naciones Unidas. La Ley Orgánica 2/2015, modificó el Código Penal, de tal forma que, actualmente, hay una respuesta penal frente a crímenes de terrorismo ya conocidas y los procedentes de nuevas amenazas.

En concreto, en el ordenamiento jurídico español existen normas procesales de aplicación directa sobre el ciberterrorismo, que deben seguir unas reglas legales, como se refiere Subijana (2008, 182), cuando dice que:

> Una primera norma significativa en materia de ciberterrorismo es la referida a la extensión de potestad jurisdiccional de los órganos judiciales que conforman el Poder Judicial. La función jurisdiccional, en cuanto ejercicio de uno de los poderes del Estado (el de juzgar y hacer ejecutar lo juzgado), requiere normalmente, cuando se trata del ejercicio del *ius puniendi*, de la existencia de conexión entre infracción y Estado.

En este sentido, la jurisdicción de los órganos judiciales y los espacios o territorios indicará el lugar donde pueden juzgar y deben ejecutar lo juzgado. Para ello, debe de haber una conexión entre la infracción y estado que puede ser de territorio, nacionalidad o protección de intereses y concretamente en el fenómeno ciberterrorismo se puede aplicar el principio de jurisdicción universal que permite al Estado actuar fuera de su territorio, independientemente de la nacionalidad de autores o víctimas.

En resumen, hemos comprobado que la aparición de las nuevas formas criminales, como la ciberdelincuencia y el ciberterrorismo, han hecho que organizaciones como la ONU y la Unión Europea (UE), y países como España, hayan tenido que adaptar su ordenamiento jurídico para garantizar la seguridad de los ciudadanos. Estas modificaciones y adaptaciones legislativas tienen que ir acompañadas de otras líneas de acción concretas, que implican crear y organizar nuevas estructuras que bajo la dirección ejecutiva de los gobiernos van poniéndose en marcha dentro de un plan estratégico integral.

Líneas de acción de España y Europa

Para finalizar este artículo haremos un resumen de las líneas de acción cibernética de países como España, que se están llevando a cabo en el ámbito de la UE. El capítulo cuarto de

la Estrategia de Seguridad Nacional española (Departamento de Seguridad Nacional, España. 2013), establece doce ámbitos prioritarios de actuación. En el ámbito de la lucha contra el terrorismo, establece diferentes líneas de acción: actuar contra el terrorismo desde su origen (prevención); disminuir nuestras vulnerabilidades (protección); hacer frente a la actividad terrorista (persecución); y preparar la respuesta para restablecer la normalidad (resiliencia). Por otra parte, en el ámbito de la ciberseguridad, marca seis líneas de acción, que van desde el incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas, hasta la intensificación de la colaboración internacional.

Por ejemplo la Estrategia de Ciberseguridad española de 2013 detalla ocho líneas de acción (Consejo de Seguridad Nacional 2013), entre las que destacamos: incrementar la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas; garantizar y fortalecer la seguridad de los sistemas de información, redes e infraestructuras críticas; potenciar las capacidades para nvestigar y perseguir las actividades terroristas; e intensificar la colaboración internacional. Tal y como indica Pastor Acosta (2009), la UE ha realizado diversos y contundentes esfuerzos en ciberdefensa, de un lado, se ha centrado en defender las infraestructuras críticas, poniendo en marcha un programa específico con el programa europeo para la protección de las infraestructuras críticas (PEPIC), apoyado con una red de alerta de las infraestructuras criticas (*critical infraestructue warninig information network*, CIWIN); y de otro lado, en la mejora de la protección de los sistemas de información y desarrollo de una vertiente legislativa que tratara de estandarizar las leyes de los países que componen la unión europea.

Así se reflejó después de los atentados de Madrid, en marzo de 2004, la primera acción en ciberdefensa, y la Comisión Europea adoptó la Comunicación sobre protección de infraestructuras críticas sobre la que España, en mayo de 2007, aprobó el Plan Nacional de Protección de Infraestructuras Críticas, creando posteriormente el CNPIC. De los esfuerzos realizados por España, específicamente en ciberdefensa, los más destacados son la labor realizada por el CCN para incrementar la Seguridad de la Información en la Administración pública, y la participación del Ministerio de Defensa como miembro del Centro de Excelencia de Ciberdefensa Cooperativa (CCD COE) de la OTAN, ubicado en Estonia.

De esta manera, como consecuencia de estos compromisos, España participa activamente en el Centro de Excelencia de Ciberdefensa Cooperativa *(CooperativeCyberDefence Centre of Excellence, CCD COE)* que la OTAN estableció en Tallín, Estonia, tras firmar el *MoU* del 14 de mayo de 2008. El CCD COE es una organización multinacional que proporciona I+D[5] y servicios de formación a la OTAN, entre otras. Además, abierta a la participación de todos los miembros de la OTAN, y con la posibilidad de firmar acuerdos con organizaciones ajenas a la OTAN, como universidades, empresas, centros, etc., centrará su trabajo en las siguientes áreas fundamentales en ciberdefensa: desarrollo de doctrinas y conceptos; formación y concienciación; investigación y desarrollo; análisis y lecciones aprendidas y consulta.

También, en el marco de la UE, se creó el Centro Europeo de Cibercrimen (EC3), de-

5 El término I+D, (en inglés R&D, research and development), se refiere a la investigación y desarrollo, que persiguen las organizaciones públicas y privadas para desarrollar nuevos productos o mejorar los existentes por medio de la investigación científica.

pendiente de Europol, que se ocupa de los delitos relacionados con ciberterrorismo, desde enero de 2013, centrándose principalmente en delitos de fraude económico, los relacionados con ataques informáticos a empresas o infraestructuras críticas y explotación sexual infantil, así como a la recogida de información de inteligencia, de gran variedad de fuentes tanto públicas como privadas a fin de alimentar una base de datos policiales, que permita facilitar información a los países miembros (Ruiz Díaz 2016). Por último, hay que indicar que este resumen de las líneas de acción que realiza España en el ámbito de la Unión Europea, tiene que realizarse con la colaboración y coordinación de todas las instituciones, tanto públicas como privadas que además tienen que estar en continua actualización y contar con el amparo legislativo necesario, si queremos hacer frente de forma global a todas las amenazas emergentes, especialmente las ciberamenazas.

Conclusiones

Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes. El ciberterrorismo, y en particular, el yihadista, se aprovecha de la existencia del ciberespacio para magnificar sus ataques y se ha convertido en la mayor pesadilla para la seguridad de las naciones occidentales. Tiene unas características tan amplias y destructivas que exige una respuesta inmediata, contundente, unida, continuada e incansable de las naciones. Nacen tantas amenazas desde cualquier lugar del mundo, la mano es tan larga y puede ser tan destructiva, que los Estados deben responder a tanto y tan rápido, que de no hacerlo, se podrían causar daños humanos, sociales y económicos irreparables.

Una vez determinados los nuevos delitos y sus penas, podemos decir que las leyes deben estar atentas a los cambios constantes de las amenazas, porque de no hacerlo los delincuentes sacarían un gran partido de ello. Así la UE y sus miembros, siguen la línea de estandarizar todo lo posible los delitos y sus legislaciones propias antiterroristas, para en consecuencia poder combatir de forma compacta y unida este germen llamado ciberterrorismo. De forma seguida, al análisis legislativo y hablando ya de las directrices defensivas, tras nuestro análisis, intuimos que para el éxito en la lucha contra el ciberterrorismo, no sirve un sistema de defensa nacional simple y convencional, además de la tecnología más moderna, se necesita un conjunto de sistemas de defensa que a su vez se unen a otros, creciendo según aumentamos fronteras, esto nos hace concluir que la ciberdefensa es un gran entramado mundial de sistemas defensivos. La UE y la OTAN tratan de marcar las directrices de esta lucha en Europa.

España como ejemplo descrito, cuenta con experiencia de años en el marco terrorista (las desarticuladas ETA y GRAPO), unas líneas estratégicas y unos marcos de cooperación con la UE, OTAN y la comunidad internacional, que son plausibles y que le permiten defenderse contundentemente dentro de sus fronteras. Tras el análisis conjunto de toda la información recopilada en este artículo, podemos decir que apoyado en la ley, el mundo civilizado ha creado un gran sistema u organigrama defensivo que crece, actualizándose continuamente, en medios económicos, humanos y tecnológicos para poder mantenerse efectivo y contrarrestar el poder destructivo de los ciberdelincuentes.

Bibliografía

Alonso García, Javier. 2015. *Derecho penal y redes sociales*. Madrid: Aranzadi.

Carlini, Agnese. 2016. "Ciberseguridad: Un nuevo desafío para la comunidad internacional", http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO67-2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf

Carta de las Naciones Unidas. 26 de junio de 1945, http://www.un.org/es/sections/uncharter/chapter-i/index.html.

CCDCOE. 2013. "NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual Process", https://ccdcoe.org/tallinn-manual.html.

Consejo de Seguridad Nacional. 2013. "Estrategia de Ciberseguridad Nacional de 2013", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf.

Conway, Maura. 2006. "Terrorism and the Internet: New Media–New Threat?". *Parliamentary Affairs 59* (2): 283-298.

Curtis E. Lemay Center. 2011. "Introduction to cyberspaceoperations", https://doctrine.af.mil/download.jsp?filename=3-12-D01-CYBER-Introduction.pdf.

Chicharro Lázaro, Alicia. 2009. "La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas". *Revista de Internet, Derecho y Política* 9 (2009): 1-14. https://dialnet.unirioja.es/servlet/articulo?codigo=3101795

_____ 2013. "La violencia terrorista en el ciberespacio: Riesgos y normativa europea sobre ciberterrorismo". En *La Sociedad Ruido/ Entre el dato y el grito*, editado por Javier Herrero et al, 80-81. La Laguna (Tenerife): Sociedad Latina de Comunicación Social. http://www.revistalatinacs.org/068/cuadernos/cac53.pdf

Departamento de Defensa, USA. 2016. "Dictionary of Military and Associated Terms. Joint Publication 1-02", https://fas.org/irp/doddir/dod/jp1_02.pdf.

Departamento de Seguridad Nacional, España. 2013. "Estrategia de Seguridad Nacional. Un proyecto compartido", http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional.

ENISA. 2017. "European Union Agency for Network and Information Security. Threat Landscape Report 2016", https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

Europol. 2013. "European Cybercrime Centre-EC3", https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

González, Miguel. 2015. "España es, tras EEUU y Reino Unido, el país que sufre más ciberataques". *El País*, 5 de febrero. http://politica.elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html.

IEEE (Instituto Español de Estudios Estratégicos). 2010. "Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio", http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf.

Instrumento de Ratificación 2001, de 23 de noviembre, del convenio sobre la ciberdelincuencia (BOE núm. 226 de 17 de septiembre de 2010). https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf.

Ministerio de Defensa, España. 2014. "Documentos de Seguridad y Defensa 60. Estrategia de la información y seguridad en el ciberespacio. Escuela de Altos Estudios de

la Defensa", http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/060_ESTRATEGIA_DE_LA_INFORMACION_Y_SEGURIDAD_EN_EL_CIBERESPACIO.pdf.

Ministerio del Interior, España. 2016. "Anuario estadístico del Ministerio del Interior 2015", http://www.interior.gob.es/documents/642317/1204854/Anuario-Estadistico-2015.pdf/03be89e1-dd38-47a2-9ce8-ccdd74659741.

Olier Arenas, Eduardo. 2013. "Inteligencia estratégica y seguridad económica". *En la inteligencia económica en un mundo globalizado*, editado por Secretaría General Técnica del Ministerio de Defensa, 9-31. Madrid: Ministerio de Defensa. Recuperado de:http://www.ieee.es/Galerias/fichero/cuadernos/CE_162_La_inteligencia_economica_en_un_mundo_globalizado.pdf

Pastor Acosta, Óscar, José Antonio Pérez Rodríguez, Daniel Arnáiz de la Torre y Pedro Taboso Ballesteros. 2009. *Seguridad nacional y ciberdefensa*. Cuadernos Cátedra ISDEFE-UPM 6. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones. http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

Ponce, Isabel. 2012. "Monográfico: Redes Sociales", http://recursostic.educacion.es/observatorio/web/ca/internet/web-20/1043-redes-sociales?showall=1.

Ruiz Díaz, Joaquín. 2016. "Ciberamenazas: ¿el terrorismo del futuro?", http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf.

Subijana Zunzunegui, Ignacio José. 2008. "El ciberterrorismo: Una perspectiva legal y judicial". Eguzkilore, 22 (2008): 169-187. http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf.

Urueña Centeno, Francisco Javier. 2015. "Ciberataques, la mayor amenaza actual", http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.