ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

“CIBERTERRORISMO E INFRAESTRUCTURAS CRÍTICAS”

AUTORÍA
MÓNICA BELÉN OLVERA GORTS
TEMÁTICA
CIENCIA, TECNOLOGÍA Y SOCIEDAD
ETAPA
BACHILLERATO

Resumen

En este artículo se plantea el ciberterrorismo como forma de agresión a la sociedad derivada del mal uso de las Tecnologías de la Información y la Comunicación (T.I.C.). Asimismo se muestran diversas acciones emprendidas por España en materia de ciberseguridad, especialmente en lo que a la protección de infraestructuras críticas (I.C.) se refiere.

Palabras clave

Seguridad, Ciberespacio, T.I.C., Valores de la Constitución española, Infraestructura Crítica, Internet, Cambio social, Unión Europea.

1. MARCO DE REFERENCIA

La Comunidad de Castilla y León mediante el DECRETO 42/2008, de 5 de junio, por el que establece su currículo de bachillerato, contempla entre sus objetivos*, “ejercer la ciudadanía democrática, desde una perspectiva global, y adquirir una conciencia cívica responsable, inspirada por los valores de la Constitución española así como por los derechos humanos”;”consolidar una madurez personal y social que les permita actuar de forma responsable y autónoma y desarrollar su espíritu crítico”; “conocer y valorar de forma crítica la contribución de la ciencia y la tecnología en el cambio de las condiciones de vida”*; *“utilizar con solvencia y responsabilidad las tecnologías de la información y la comunicación”*. Añade en su anexo respecto a la materia de Física que, *“todo un conjunto de artefactos presentes en nuestra vida cotidiana están relacionados con avances en este campo del conocimiento, que han supuesto una fuente de cambio social, han influido en el desarrollo de las ideas y han tenido implicaciones en el medio ambiente”*. Establece entre sus objetivos: *“Comprender las complejas interacciones actuales de la Física con la tecnología, la sociedad y el ambiente, valorando la necesidad de trabajar para lograr un futuro sostenible y satisfactorio para el conjunto de la humanidad.”.*

Este artículo plantea una propuesta curricular en el ámbito de la interacción entre Ciencia, Tecnología y Sociedad. En primer lugar, se muestra el impacto del mal uso de las nuevas tecnologías de información

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

y comunicación, en la seguridad individual y colectiva a escala mundial; en segundo lugar, se presenta el concepto de Infraestructura Crítica, como realidad soporte de nuestro estilo de vida actual y el concepto de ciberterrorismo, como forma de agresión a la misma; finalmente se expone una pequeña muestra de la respuesta española en el ámbito de la ciberseguridad.

2. PRESENTACIÓN DEL PROBLEMA.

Año 1985, Japón.
El grupo terrorista conocido como *Middle Core Faction* ataca el sistema que controla los ferrocarriles de alta velocidad japoneses. Para ello, en primer lugar, cortan el suministro eléctrico y los cables de control informatizados del ferrocarril, y posteriormente, interceptan y perturban las radiocomunicaciones de la Policía para anticipar y ralentizar la capacidad de respuesta de las autoridades.
Aunque nadie resultó herido con la acción, afectó a 6,5 millones de usuarios y le costó a la compañía aproximadamente seis millones de dólares.

Década de los 90:

El grupo guerrillero tamil, *Liberation Tigers*, ataca, a través de Internet, objetivos estadounidenses lanzando un mailbombing contra organizaciones gubernamentales.

Guerra del Golfo. Aviones armados con municiones de precisión atacan la red de telecomunicaciones y energía eléctrica de Bagdad.
Según los medios de comunicación, alguien penetró en los servidores militares estadounidenses y alteró los archivos médicos de los soldados. Entre otras cosas, cambiaron los tipos de sangre, información crucial para una transfusión durante una batalla.

Guerra entre Serbia y Croacia. El grupo de hackers serbios *Black Hand* ataca el Centro de Informática de Kosovo, universidades y la versión en línea del periódico *Vjesnik*. La respuesta croata es entrar en el sitio web de la Biblioteca Serbia. *Black* Hand roba el fichero de contraseñas del Rudjer Boskovic Institute como reacción. Seguidamente, los hackers croatas se introducen en dos servidores serbios.

Guerra de Kosovo. Hackers rusos, yugoslavos, norteamericanos, llenaron páginas de graffitis a favor y en contra de Milosevic o la OTAN.
La red se utilizó para poner en contacto a los de dentro y los de fuera del territorio. Nacieron nuevos foros de discusión, la información de la guerra volaron por las listas, discutiéndose en ellos todos los sucesos acontecidos. La red se llenó de propaganda.

Año 2005, España.
Se detiene en Málaga a un hacker por atacar a través de Internet un ordenador del departamento de Defensa de Estados Unidos que comprometía la seguridad de un dique seco de mantenimiento de submarinos nucleares en la base naval de "Point Loma", San Diego, California.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

Año 2007, Estonia.
Las páginas oficiales de varios departamentos estonios, las del Gobierno y las del gobernante Partido de las Reforma, quedaron paralizadas por ataques informáticos provenientes del exterior. Al mismo tiempo los sistemas de algunos bancos y periódicos resultaron bloqueados durante varias horas por una serie de ataques distribuidos de denegación de servicio.

Año 2007, EEUU.
Una red informática del Pentágono sufre un ataque lanzado por hackers desde China que se convirte en “uno de los ciberataques de más éxito” al Departamento de Defensa de Estados Unidos. Aunque es cuestionable la cantidad de información confidencial que se robó, el incidente aumentó el nivel de preocupación, al poner de relieve cómo se podían interrumpir sistemas en momentos críticos.

12 de Septiembre de 2008.
El CERN reconoce que un grupo hacker griego, llamado *Greek Security Team (*GTS), ha vulnerado la seguridad de su sistema informático.

Año 2008, India.
El Centro Nacional de Informática del país denuncia que sufre, desde hace 18 meses, ataques desde conexiones telefónicas a Internet en China. Destacados miembros del Servicio de Inteligencia afirmaron que los hackers accedieron a las cuentas de correo electrónico de 200 ministros, burócratas y funcionarios de defensa, y continuaron atacando servidores indios al ritmo de tres o cuatro al día

26 de septiembre del 2010, Irán.
Un sofisticado virus informático infecta varias computadoras en la primera estación nuclear de Irán, según informó la agencia de noticias oficial iraní (IRNA). El virus, conocido como Stuxnet, es capaz de hacerse con el control de fábricas y plantas industriales.
Expertos creen que su complejidad indica que no fue desarrollado por un hacker solitario, sino por una potente organización.

En esa misma fecha, los responsables de la página web Twitter.com reconocieron que ésta quedó prácticamente inutilizada tras un fallo de seguridad XSS o Cross-scripting, que permitió la inserción de JavaScript malicioso. Twitter necesitó “cerrar” sus servicios durante varias horas para restablecer sus sistemas.

5 de noviembre de 2010, España.
En una entrevista a los medios, un alto responsable del Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia, reconoce que en lo que va de año, España ha sufrido más de 80 ataques cibernéticos graves contra instituciones, organizaciones e infraestructuras críticas, y en algún caso el objetivo ha sido el propio Centro.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

Estos hechos son una pequeña muestra de los nuevos tipos de agresiones que se vienen observando desde los años 80 a nivel mundial. Todos tienen como común denominador la presencia de las T.I.C. o/y de servicios públicos estatales y privados, bien como objetivo, bien como medio o instrumento del ataque.

A escala europea es de reseñar la importancia de las denominadas Infraestructuras Críticas como objetivos de ataque. La Comunicación de la Comisión al Consejo y al Parlamento Europeo de 20 de Octubre de 2004, sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, define este término como *"aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros".*

A través de diversos comunicados, la Unión Europea afirma ser consciente de que las infraestructuras críticas europeas están muy interconectadas, y que son sumamente interdependientes al depender cada vez más de tecnologías de la información como Internet, la radionavegación y la comunicación por satélite. Asimismo, reconoce que estos hechos las hacen muy vulnerables, en particular, a ataques ciberterroristas. Considera de vital importancia la gestión eficaz de la seguridad de las mismas por parte de los Estados miembro.

Por tanto, es necesario estudiar este fenómeno en profundidad. Las agresiones y amenazas existentes en el ciberespacio son muchas y muy variadas, y todos ellas conforman lo que se denomina delincuencia informática o ciberdelincuencia. De todos ellas, el ciberterrorismo se presenta como una gran amenaza en cuanto a su relación con las Infraestructuras Críticas se refiere. Antes de desarrollar este último aspecto es necesario presentar el concepto de ciberterrorismo.

3. CONCEPTO DE CIBERTERRORISMO.

Con el desarrollo de las T.I.C. y su inclusión en nuestra vida diaria, ha aparecido una nueva dimensión desde donde la amenaza y la agresión pueden surgir, el ciberespacio.

Pero, ¿qué es el ciberespacio?

Existe variedad de definiciones:

En el ámbito TIC, el ciberespacio es "*el conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos".*

También puede definirse como *"un conjunto de sistemas de información interconectados, dependientes del tiempo junto con los usuarios que interactúan con estos sistemas".*

Otra posible definición es *"aquel ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura crítica asociada. El ciberespacio se puede considerar como la interconexión de los seres*

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física".

El Departamento de Defensa de los EEUU considera el ciberespacio como *"un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de TI, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos y controladores".*

Para la Comisión Europea el ciberespacio comprende *"el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo*".

Es claro que no existe consenso sobre qué es el ciberespacio, con todas las dificultades e implicaciones legales que esto conlleva en el marco internacional de tomas de posiciones comunes. Con todo, lo que sí parece evidente es que ha aparecido un nuevo teatro de operaciones que es necesario estudiar.

Si se considera el ciberespacio como un lugar inmaterial asociado a una colección de recursos, es claro que los actores implicados (individuos, grupos, organizaciones, negocios, Estados) pueden competir por controlarlo de múltiples formas y con variedad de fines. Esto conduce inevitablemente a confrontaciones en el ciberespacio y al concepto de ciberconflicto. Se entenderá entonces por ciberconflicto, una confrontación entre dos o más partes, donde una de ellas, al menos, ataca a la otra mediante ciberataques.

¿Y de qué manera, cómo se puede efectuar un ataque en el ciberespacio? Para realizar un ciberataque se necesita un arma o elemento de ataque, un medio para hacer llegar dicho elemento al objetivo y una puerta de entrada al mismo. Veamos brevemente cada uno de ellos.

Algunos de los elementos de ataque más conocidos, cuya definición figura en una de las guías del CCN-CERT son:

Virus: Programa diseñado para infectar otros programas o ficheros copiándose a sí mismo dentro de ellos.

Código dañino o malware: Software capaz de realizar un proceso no autorizado sobre un sistema con el propósito de ser perjudicial.

Troyano: Programa que no se replica ni hace copias de sí mismo, pero permite intrusiones, borrar datos, etc.

Gusano: Programa que se replica a sí mismo infectando a otros ordenadores y propagándose automáticamente en una red independientemente de la acción humana.

En cuanto a los métodos de entrega, hay muchos, los más usuales son: correos electrónicos, sitios web con enlaces o descargas infectadas, falsificación de elementos hardware, software o componentes electrónicos, etc.

Las puertas de entrada normalmente son las vulnerabilidades del ordenador, sistema o red objetivo; brechas de seguridad en códigos, aplicaciones y configuración, pueden permitir un acceso remoto no autorizado al objetivo y controlarlo.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

Hasta ahora se ha definido el lugar donde se realiza o puede efectuarse el ataque, el acto cometido y los elementos necesarios para realizarlo. Se ha hecho referencia también a los tipos de agentes que pueden realizar la amenaza y/o agresión.

Para dar el salto al concepto de ciberterrorismo haremos varias consideraciones:

En primer lugar es necesario calificar la agresión o amenaza realizada en el ciberespacio como una acción terrorista.

En segundo lugar es necesario calificar al agente o agentes de la acción terrorista como terroristas.

Por último, puesto que las finalidades de las acciones terroristas son variadas, así como también lo son los recursos necesarios para cometer el ataque o amenazar con hacerlo, el ciberterrorismo necesariamente comprenderá diferentes modalidades.

En consecuencia, para aplicar adecuadamente el concepto de ciberterrorismo a una situación determinada es necesario estudiar:

- El escenario donde se realiza la acción.
- El agente que realiza el acto.
- El tipo de acto.
- La finalidad del acto.
- Los medios utilizados.
- El objetivo de la acción.

¿Y cuál es la terminología aceptada por la Comunidad Internacional?

Puesto que no existe consenso global ni en la definición de terrorismo, ni en la definición de ciberespacio, es imposible la existencia de un concepto universal de ciberterrorismo. No existe un ciberterrorismo único a escala internacional.

A efectos de este artículo, se adoptará la definición de ciberterrorismo con la que trabaja la Guardia Civil española: *"El empleo de las TIC, por parte de grupos terroristas para la consecución de sus objetivos; utilizando Internet como* ***instrumento o medio de comisión del delito, o*** *como* ***acción del delito".*** Esta doble vertiente del concepto engloba tanto la utilización de las TIC y más concretamente Internet como elemento de apoyo a la infraestructura de sus organizaciones (comunicaciones, apología y propaganda, recluta, financiación, etc...) y como objetivo de la acción directa (ataques informáticos contra objetivos tecnológicos tales como operadores de telecomunicaciones, infraestructuras críticas, etc...).

En particular se hablará de ciberterrorismo amplio, si se utiliza Internet como instrumento o medio, o de ciberterrorismo estricto si Internet es el objeto de ataque o acción del delito.

La siguiente cuestión a desarrollar es la relación existente entre Internet y las Infraestructuras Críticas. El nexo es claro.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

3. INFRAESTRUCTURAS CRÍTICAS E INTERNET.

En la sociedad actual la mayoría de las infraestructuras que dan soporte a nuestro estilo de vida, al desarrollo del estado del bienestar, se apoyan, tanto para la gestión interna como para la provisión de servicios, en el ciberespacio, y en particular, en Internet y en sistemas de control industrial.

En efecto: en la gestión de datos, supervisión y control de variables de proceso de muchas infraestructuras se utilizan determinados sistemas de control industrial llamados comúnmente SCADA (Supervisory Control And Dato Acquisition). Así, los sistemas SCADA están presentes en fábricas químicas, redes eléctricas, centrales de generación eléctrica, industrias de petróleo y gas, tratamiento de agua y residuos, industrias farmacéuticas, centrales nucleares, oleoductos, plataformas petroleras, entre otras. Pero ¿qué tienen de especial que entrañe tanto riesgo? Estos sistemas tienen la particularidad de estar configurados para ser accesibles por los individuos pertinentes a larga distancia, mediante un servidor Web que utilice Internet como red de comunicación entre ellos. El acceso al sistema para poder modificar parámetros del proceso industrial en cuestión, obtener datos, etc., es rápido y barato desde cualquier punto del planeta con tal de tener un punto de conexión a la red y un ordenador.

El desconocimiento por parte del propietario de este tipo de interconexión de los sistemas SCADA, la ausencia de buenas prácticas de seguridad como la realización de actualizaciones periódicas de los sistemas de seguridad o una adecuada gestión de las contraseñas, aumentan los riesgos de seguridad facilitando realizar acciones remotas que permiten el control de los mismos.

Si un acto ciberterrorista afectara a alguna de estas infraestructuras la seguridad de cualquier nación y de las gentes que viven en ella, podría verse comprometida. Por tanto es de importancia fundamental tomar las medidas que sean necesarias para prevenir la materialización de esta amenaza.

Como se ha puesto de manifiesto, la inclusión de las T.I.C. en nuestra forma de vida actual ha conllevado la apertura de la puerta a otra realidad: el ciberespacio. Y con él, la posibilidad de agredir y amenazar de forma novedosa hasta ahora. La comunidad internacional ha asumido esta realidad y ha decidido enfrentarse a ella. Los dirigentes de los países deben de liderar la lucha contra este nuevo frente. Y esta lucha pasa por revisar y modificar los conceptos tradicionales de seguridad y defensa.

4. CIBERESPACIO Y SEGURIDAD NACIONAL.

Tradicionalmente se ha entendido por seguridad nacional el elemento garante de la independencia, soberanía e integridad de una nación. Las amenazas o agresiones a esta seguridad provenían del mar, cielo o tierra. La defensa nacional se desarrollaba en el espacio y en el tiempo.

La inclusión del ciberespacio como nueva dimensión a considerar junto con el espacio y el tiempo, aconsejan que Seguridad y Defensa nacionales deban de ser enfrentadas de diferente modo. Ya no

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

basta con proteger territorio, intereses y ciudadanos. La protección ha de extenderse también a organizaciones públicas y privadas, en especial a las Infraestructuras Críticas. Recordemos que las Infraestructuras Críticas son el soporte de nuestro estilo de vida actual.
Todos estos elementos son "blancos" para una agresión o amenaza desde el ciberespacio.

Son necesarias por tanto, nuevas políticas de seguridad y defensa donde la ciberseguridad esté contemplada en las estrategias nacionales de seguridad y desarrolladas mediante los planes estratégicos pertinentes.

España tiene una larga tradición en lo que se refiere a la defensa contra todo aquello que amenace o agreda los valores y principios propugnados en su Constitución. Adaptándose a las necesidades de la situación, ha ido haciendo frente al terrorismo, la delincuencia organizada y la delincuencia informática.

Los esfuerzos realizados en materia de ciberseguridad no se pueden enmarcar en ámbitos más o menos prediseñados y específicos. Son múltiples y de diversos calados las iniciativas desarrolladas en este tema: De un lado, legislación, planes y estrategias; de otro, actuaciones e iniciativas de diversos ministerios, organismos y organizaciones gubernamentales. Presentar una visión general de todas ellas excede el objetivo de este artículo. Sin embargo, para ilustrar la reacción de España en el ámbito de seguridad y defensa, ante los efectos destructivos del ciberterrorismo, se expone documentación relativa a la consideración del ciberespacio como elemento constitutivo del "campo de batalla" y los distintos objetivos nacionales cuya seguridad es necesario mantener.

4.1. Seguridad y prioridades estratégicas nacionales.

En el **preámbulo de la Constitución** de 1978 se hace la primera mención a la seguridad y los elementos que han de gozar de la misma: "L*a Nación española, deseando establecer la justicia, la libertad y* ***la seguridad*** *y promover el bien de cuantos la integran, en uso de su soberanía, proclama su voluntad de: Garantizar la convivencia democrática dentro de la Constitución y de las leyes conforme a un orden económico y social justo. Proteger a todos los españoles y pueblos de España en el ejercicio de los derechos humanos, sus culturas y tradiciones, lenguas e instituciones.".*

El **Libro Blanco de la Defensa** del año 2000, en su capítulo I establece el panorama de riesgos español, donde menciona la globalización del escenario estratégico: ***"****Los prodigiosos avances registrados en los campos de las* ***comunicaciones y de los sistemas de información****, los flujos de capitales e inversiones y las relaciones comerciales de extensión mundial han favorecido la integración de los mercados financieros y estimulado la circulación de ideas, personas y bienes. El mundo se ha hecho más pequeño y el proceso de globalización parece irreversible".*

Vislumbra un campo de batalla más amplio del que el ciberespacio forma parte:
"Conceptos como campo de batalla terrestre, ámbito marítimo o espacio aéreo han evolucionado en los últimos años hasta su integración en un único espacio de batalla que, además de los entornos

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

precedentes, comprende también el espectro electromagnético y la noción moderna de ciberespacio e, incluso, el dilatado campo en el que se desenvuelve la comunicación social"

Clasifica las prioridades estratégicas nacionales a defender estableciendo dos categorías mediante las que se amplían los objetivos a proteger a los que hace referencia la Constitución:
"Los intereses nacionales de seguridad se pueden agrupar, de forma muy general y como se explica en los párrafos siguientes, en dos categorías: vitales y estratégicos
Los intereses vitales son, en realidad, los elementos constitutivos del Estado que deben preservarse de cualquier agresión: el territorio peninsular y extrapeninsular con sus accesos aéreos y marítimos, la población, el ordenamiento constitucional, la soberanía y la independencia.
Son intereses estratégicos aquellos que aportan seguridad a nuestro entorno y cuya protección contribuye decisivamente a la defensa de los intereses vitales. Destacan entre ellos los que se derivan de la situación geográfica y condición marítima de España".

La **Revisión Estratégica de la Defensa** del año 2003, en su Planteamiento General establece los intereses nacionales y riegos para la seguridad. Hace mención a la vulnerabilidad de las infraestructuras críticas y considera, entre otros, los ataques cibernéticos:
"La economía mundial, fuertemente globalizada, depende del intercambio amplio de información, cuya interrupción provocaría problemas comparables a los ocasionados por la alteración del flujo de los recursos básicos. La vulnerabilidad estratégica que supone este tipo de amenazas comprende especialmente dos campos. Por un lado, los ataques contra los sistemas que regulan infraestructuras básicas para el funcionamiento de un país –como el sabotaje de los servicios públicos, la paralización de la red de transporte ferroviario o la interrupción de la energía eléctrica a una gran ciudad– suponen un serio quebranto para la normalidad y la seguridad de una sociedad avanzada. En consecuencia, todas las infraestructuras básicas deben dotarse de elementos de protección suficientes para poder neutralizar este tipo de agresiones cuando su funcionamiento depende de complejos sistemas informáticos y de comunicaciones.
Por otro lado, la penetración en la red de comunicación, mando y control de las crisis o en las bases de datos de los servicios de inteligencia puede suponer una amenaza directa a la seguridad nacional. Por tanto, las Fuerzas Armadas deben dotarse de las capacidades necesarias para impedir cualquier tipo de agresión cibernética que pueda amenazar la seguridad nacional".

Ambos documentos no tuvieron continuidad.

La **Ley Orgánica 5/2005** de 17 de Noviembre de la Defensa Nacional, no introduce ninguna modificación respecto a la versión tradicional de prioridad nacional y dimensiones del escenario estratégico español. Afirma:
"…El escenario estratégico ha visto desaparecer la política de bloques que protagonizó la guerra fría y emerger la globalización y un nuevo marco en las relaciones internacionales. Al mismo tiempo, junto a los riesgos y amenazas surgen otros como el terrorismo transnacional con disposición y capacidad de infligir daño indiscriminadamente…".
"*Las operaciones desarrolladas por las Fuerzas Armadas pueden ser:*

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

…La vigilancia de los espacios marítimos, como contribución a la acción del Estado en la mar, la vigilancia del espacio aéreo y el control del espacio aéreo de soberanía nacional y aquellas otras actividades destinadas a garantizar la soberanía e independencia de España, así como a proteger la vida de su población y sus intereses".

No menciona en ningún momento la problemática derivada del mal uso del ciberespacio.

La **Directiva de Defensa Nacional 1/2008** reconoce los riesgos derivados de la existencia y actividad humana en el ciberespacio, así como la necesidad de proteger sus intereses vitales. Menciona además la importancia de establecer medidas multidisciplinares e integrales en el ámbito de la seguridad y defensa nacional**:**
"La revolución tecnológica de la llamada Era de la información ha introducido una dimensión nueva en el ámbito de la seguridad y defensa, el ciberespacio, generando vulnerabilidades que pueden interrumpir o condicionar el normal funcionamiento de la sociedad".
"España defiende como intereses esenciales la soberanía, la integridad territorial y el ordenamiento constitucional, así como asegurar la libertad, la vida y la prosperidad de sus ciudadanos."
"La seguridad y la defensa son competencias que el Estado garantiza mediante la integración de distintos instrumentos y políticas. No se trata, por tanto, de una responsabilidad asumida únicamente por el Ministerio de Defensa, sino que exige un enfoque multidisciplinar y una actuación integral del conjunto de las administraciones públicas competentes, así como la confluencia de instrumentos civiles y militares, públicos y privados".

La **Estrategia de Seguridad Nacional** de 2011 que lleva por nombre "Estrategia Española de Seguridad. Una responsabilidad de todos", contempla las cuestiones de la ciberseguridad y la protección de las infraestructuras críticas como objetivos estratégicos a defender. Expone las medidas efectuadas en estas materias relativas a la prevención y respuesta a la amenaza, así como las líneas de acción de trabajo en el futuro:
"Los ciberataques más comunes tienen fines comerciales, pero también estamos expuestos a agresiones por parte de grupos criminales, terroristas u otros, incluso de Estados. Las nuevas tecnologías de información y comunicación ofrecen nuevos y más sofisticados medios para el espionaje y la contrainteligencia. Mejorar la seguridad en el ciberespacio pasa por fortalecer la legislación, reforzar la capacidad de resistencia y recuperación de los sistemas de gestión y comunicación de las infraestructuras y los servicios críticos, y por fomentar la colaboración público-privada con este fin. Es necesaria la coordinación de los diversos agentes involucrados, así como impulsar la cooperación internacional con el objetivo de desarrollar acuerdos de control de las ciberamenazas"

El **Real Decreto 1097/2011** de 22 de Julio, por el que se aprueba el Protocolo de Intervención de la Unidad Militar de Emergencias, incluye en su articulado a las infraestructuras críticas como elementos prioritarios a defender:
"La intervención de la UME podrá ser ordenada cuando alguna de las siguientes situaciones de emergencia se produzca con carácter grave, independientemente de que se trate de una emergencia de interés nacional o no: …Las que sean consecuencia de atentados terroristas o actos ilícitos y

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

violentos, incluyendo aquéllos contra infraestructuras críticas, instalaciones peligrosas o con agentes nucleares, biológicos, radiológicos o químicos".

La **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, es de singular importancia. Este documento está encuadrado en el marco comunitario generado por la Comunicación de la Comisión de 12 de Diciembre de 2006, "Programa Europeo para la Protección de Infraestructuras Críticas" (COM (2006) 786 final) y la Directiva 2008/114/CE de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Entre otros temas aborda:

- Establecer la responsabilidad de asegurar la protección de las Infraestructuras Críticas Españolas en los Estados miembros y las gestores/operadores de las mismas.
- Centrar esta protección principalmente en las amenazas y agresiones deliberadas, y con carácter especial, en las de tipo terrorista.
- La dependencia creciente de las infraestructuras críticas de las tecnologías de la información, tanto en su gestión, como en su vinculación con otros sistemas.
- El establecimiento de medidas de protección adecuadas y la regulación de la colaboración coordinada de todos los actores implicados en las IC: Ministerio del Interior, otros ministerios y órganos de la Administración General del estado y de otras Administraciones, organismos públicos y sector privado.

El **Real Decreto 704/2011**, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, es el reglamento ejecutor de la Ley 8/2011 por la que se establecen medidas de protección de las IC. Desarrolla el marco previsto por dicha Ley, concretando las actuaciones de los distintos órganos integrantes del Sistema de Protección de Infraestructuras Críticas, así como los diferentes instrumentos de planificación del mismo. Asimismo regula las obligaciones que deben asumir tanto el Estado como los operadores de las Infraestructuras Críticas.

BIBLIOGRAFÍA

Fojón, Enrique; Sanz, Ángel, 2010.
"Ciberseguridad en España: una propuesta para su gestión", Análisis del Real Instituto Elcano, ARI nº 101/2010

Ottis Rain, Lorents Peeter. Cooperativa Cyber Defence Centre of Excellence, 2010
"Cyberspace: Definitions and Implications" Tallinn, Estonia.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

Cuadernos de Estrategia. “Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio”. Ministerio de Defensa. 2010.

Real Decreto 1097/2011 de 22 de Julio, por el que se aprueba el Protocolo de Intervención de la Unidad Militar de Emergencias

Estrategia de Seguridad Nacional de 2011, “Estrategia Española de Seguridad”

Directiva de Defensa Nacional 1/2008

Ley Orgánica 5/2005 de 17 de Noviembre de la Defensa Nacional

Revisión Estratégica de la Defensa del año 2003

Libro Blanco de la Defensa del año 2000.

Constitución española de 1978.

Comunicación de la Comisión al Consejo y al Parlamento Europeo de 20 de Octubre de 2004, sobre protección de las infraestructuras críticas en la lucha contra el terrorismo.

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas

WEBGRAFÍA

www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401Glosario_y_abreviaturas/401/index.html

www.revista-ays.com/DocsNum01/SeguridadEstado/GuardiaCivil.pdf

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 60 – JUNIO DE 2013

Autoría

- Nombre y Apellidos: Mónica Belén Olvera Gorts
- Centro, localidad, provincia:
- E-mail: monicaolveragorts@yahoo.es