CAPÍTULO PRIMERO

ALCANCE Y ÁMBITO DE LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

ALCANCE Y ÁMBITO DE LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

María José Caro Bejarano

RESUMEN

En un mundo necesitado de seguridad surge una nueva dimensión con el llamado ciberespacio. Es un nuevo campo de batalla en el siglo XXI, sin fronteras y asimétrico. Así surgen nuevos términos con el prefijo ciber-. Este capítulo trata varias definiciones de ciberespacio y sus implicaciones en la sociedad actual. Se describen las iniciativas españolas en materia de seguridad relacionadas con las Tecnologías de la Información y las Comunicaciones, así como la gestión de esa seguridad. Se describe brevemente el ámbito europeo, de la OTAN y el norteamericano. Los diferentes tipos de ataques y atacantes son analizados, así como la evolución en el diseño de las ciberarmas, desde el código dañino hasta llegar al empleo de metodologías formales para desarrollar código. Se mencionan especialmente las amenazas a las infraestructuras críticas. Surge entonces la necesidad de las estrategias de ciberseguridad con dos posturas nacionales diferentes respecto al riesgo en el ciberespacio: unas se han planteado con carácter defensivo y otros con carácter ofensivo.

Palabras clave: Seguridad, ciberespacio, tecnologías, información, comunicaciones, amenaza, estrategia, ataques, redes, internet, ciberseguridad, ciberdelincuencia, ciberataque, ciberdefensa, ciberterrorismo, ciberarma, vulnerabilidad, infraestructura crítica.

NATIONAL SECURITY SCOPE IN CYBERSPACE

ABSTRACT

In a world claiming for security, a new dimension arises with the so-called cyberspace. It is a new battle field in the XXI century, without borders and asymmetric. Therefore, there are new words with the cyber- prefix. This chapter addresses several cyberspace definitions and its implications in the current society. Spanish security initiatives related to Information and Communication Technologies are described; and also the management of that security is described. European, NATO and USA scopes are pointed out. The different attacks and attackers types as well as the cyberarms design evolution are analysed, from malicious code to the use of formal methodologies in order to develop code. The threats on critical infrastructures are specially mentioned. Then, the need of cybersecurity strategies arises regarding the risk on cyberspace: some of them are planned with defensive character whereas others are planned with offensive character.

Key words: Security, cyber space, technology, information, communications, threats, strategy, attacks, networks, Internet, cyber security, cyber crime, cyber attack, cyber defence, cyber terrorism, ciber arm, vulnerability, critical infrastructure.

INTRODUCCIÓN

Los conceptos de seguridad nacional y ciberespacio son de uso generalizado por parte de amplios sectores de nuestra sociedad. Sería interesante pues, previamente a entrar en materia, intentar dar una definición clara de Seguridad, Seguridad Nacional y Ciberespacio.

La palabra seguridad se puede aplicar a muchos ámbitos. Así se habla de seguridad física, seguridad vial, seguridad ciudadana, seguridad jurídica, seguridad económica, seguridad energética, seguridad financiera, seguridad de las tecnologías de la información, etc., cuya gestión es la responsabilidad de diferentes ministerios, sin embargo, en este contexto, la seguridad nacional es aquella encargada de proteger los intereses nacionales.

Tradicionalmente la seguridad nacional se ha concebido como el elemento garante de la identidad y supervivencia nacionales o, dicho de

otra forma, de su independencia e integridad. No obstante, este concepto se ha ido ampliando incluyendo actualmente un mayor número de riesgos, entre los que figuran por ejemplo, los desastres naturales, el cambio climático, las tecnologías de la información y las comunicaciones. Todo ello según la apreciación de su dimensión por la población.

En el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Si antes en el ámbito de la defensa estaba claro que nos movíamos en las tres dimensiones de tierra, mar y aire, e incluso el espacio, ahora contamos con una dimensión adicional, y más intangible que las anteriores.

Existe cierta dificultad para comprender y explicar qué es el ciberespacio; por una parte, depende de la perspectiva y por otra parte, se cae en el error de querer definir este término basándose en conceptos antiguos.

Dentro de la comunidad TIC (Tecnologías de la Información y Comunicaciones) el ciberespacio se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos (1).

El ciberespacio puede también puede definirse como «un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas» (2).

Otra posible definición de ciberespacio es: *«un 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 física asociada. El ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física»* (3).

Muy frecuentemente se identifica Internet con ciberespacio, aunque, el ciberespacio es un concepto mucho más amplio. Por tanto, resulta más adecuado referirse, por ejemplo, al *ciberterrorismo* con expresiones como «terrorismo por medios informáticos», «teleterrorismo» o «terroris-

(1) Fojón Enrique y Sanz Ángel. «*Ciberseguridad en España: una propuesta para su gestión*», Análisis del Real Instituto Elcano, ARI Nº 101/2010

(2) Rain, Ottis and Lorents Peeter. «*Cyberspace: Definitions and Implications*», Cooperativa Cyber Defence Centre of Excellence, Tallinn, Estonia. 2010.

(3) Definición extraída del glosario de términos informáticos, *Whatis*. Enlace: http://whatis.techtarget.com/.Fecha de consulta 5.9.2010.

mo digital» (4). Sin embargo, la utilización de expresiones como *ciberdelincuencia* o *ciberterrorismo* como sinónimas, en el primer caso de «delincuencia vía internet» o en el caso de la segunda, de «terrorismo a través de la red», han generado en el colectivo la identificación de ciberespacio e Internet como ese mismo *lugar intangible* al que anteriormente se hacía mención.

La principal característica que ha contribuido al desarrollo y a la dependencia del ciberespacio es el *tratamiento de la información*. En la llamada *sociedad de la información o cibersociedad* (5), la premisa es que la información por sí misma tiene un valor susceptible de generar poder (político, económico, social, etc.). Cuanto mayor sea la eficacia con que sea manejada y tratada aquélla, mayores serán los beneficios.

El ciberespacio ha experimentado un enorme y veloz desarrollo, así como la dependencia que nuestra sociedad tiene de él, lo que contrasta con el menor y lento avance en materias de *ciberseguridad*. Por este motivo, los actores (tanto estatales como no estatales) que decidan operar en el ciberespacio, obtendrán una serie de ventajas asimétricas, como son las siguientes (6):

- El ciberespacio es un «campo de batalla» de grandes dimensiones y donde resulta relativamente fácil asegurar el anonimato. Los ataques se pueden lanzar desde casi cualquier parte del mundo.
- Los efectos de los ataques son desproporcionados con respecto a su coste. Las operaciones se pueden realizar sin necesidad de efectuar fuertes inversiones en recursos humanos y materiales.
- La naturaleza de los ciberataques fuerza a la mayoría de las víctimas, tanto reales como potenciales, a adoptar una actitud defensiva.
- Esta amenaza tiene un alcance global, en la cual el actor (ya sea ciberdelincuente, ciberterrorista, etc.), puede operar desde cualquier parte del mundo con el único requisito de tener acceso al ciberespacio. La conexión al ciberespacio de cualquier sistema lo convierte en un objetivo susceptible de ser atacado.

---

(4) Masana, Sebastián. «*El ciberterrorismo: ¿una amenaza real para la paz mundial?»,* Tutor: Carlos Escudé. Facultad Latinoamericana de Ciencias Sociales, 2002.

(5) Joyanes, Luis. «*Cibersociedad. Los retos sociales ante un nuevo mundo digital*». Ed. McGraw-Hill. 1997.

(6) Umphress, David A. «*El Ciberespacio. ¿Un aire y un espacio nuevo?», Air & Space Power Journa*l. Tercer Trimestre 2007. Enlace: http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2007/3tri07/umphress.html. Fecha consulta 7.9.2010.

– Proporciona las herramientas necesarias para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos (7).

Por tanto, al movernos en la sociedad de la información o también llamada cibersociedad, surgen nuevos términos con el prefijo ciber para denominar eventos que se producen en el ciberespacio. De ahí surgen los términos: ciberentorno, ciberactivismo, ciberdelincuencia, ciberterrorismo, ciberamenaza, ciberguerra, ciberrebelión, ciberejército, ciberarma, etc.

Nos enfrentamos a un nuevo campo de batalla dentro de la seguridad que es el ciberespacio, donde se producen comportamientos o fenómenos ya conocidos, pero empleando técnicas nuevas; y también fenómenos nuevos que surgen de la propia idiosincrasia del ciberespacio y en donde, en ocasiones, no están claras las fronteras entre activismo y delincuencia (8).

El ciberespacio no tiene fronteras, es un nuevo campo de batalla del siglo XXI, aunque ya se intuyó a finales del siglo XX. El campo de batalla o teatro de operaciones es el ciberespacio, los atacantes son los hackers que utilizan un armamento no siempre sofisticado que es el código dañino.

CIBERESPACIO: DEFINICIONES E IMPLICACIONES

Definiciones

En los últimos años el término «ciber» se ha usado para describir casi todo lo que tiene que ver con ordenadores y redes y especialmente en el campo de la seguridad. Un campo de estudio emergente está mirando a los conflictos en el ciberespacio, incluyendo las ciberguerras entre estados, el ciberterrorismo, los ciberejércitos, etc. Desafortunadamente, sin embargo, no existe un consenso sobre qué es el ciberespacio, por no decir de las implicaciones de los conflictos en el ciberespacio (9).

---

(7) Sánchez Medero, Gema. «*Ciberguerra y ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica*». Amérigo Cuervo-Arango, Fernando; Peñaranda Algar, Julio. «*Dos décadas de Posguerra Fría*». Instituto Universitario General Gutiérrez Mellado, 2009. Tomo I, p. 215-241.

(8) ¿Ciberactivistas o ciberdelincuentes? Los ataques que tumbaron las webs de la SGAE y Cultura dividen Internet –Para unos son vandalismo y para otros una nueva forma de protesta– En breve serán delito en España. ELPAIS.com. 20.10.2010.

(9) Ottis, Rain and Lorents, Peeter. «*Cyberspace: definition and implications*». Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2010.

El término ciber ha evolucionado desde el trabajo de Norbert Wiener, que definió el término cibernética en su libro «Control y comunicación en el animal y en la máquina» (Wiener 1948). La idea de que los humanos puedan interactuar con máquinas y que el sistema resultante proporcione un entorno alternativo de interacción proporciona la base del concepto de ciberespacio.

A principio de los años 80 el autor de ciencia ficción William Gibson dio el siguiente paso al acuñar el término ciberespacio en uno de sus libros (10). A pesar de ello, esta palabra se ha extendido en los círculos profesionales y académicos. Durante años se han dado muchas y diferentes definiciones para el ciberespacio. El Departamento de Defensa de 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» (11).

La Comisión Europea define vagamente el ciberespacio como «el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo» (12).

La UIT, Unión Internacional de Telecomunicaciones, define el ciberespacio como el lugar creado a través de la interconexión de sistemas de ordenador mediante Internet. Define también conceptos como ciberentorno y ciberseguridad. El ciberentorno (13) incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes. La ciberseguridad es definida como «el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utili-

(10) Gibson, William. «*El Neuromante*». (1984).

(11) Joint Publication 1-02. Department of Defense. Dictionary of Military and Associated terms. (2009) [on line], http://www.dtic.mil. Fecha consulta 3.11.2009

(12) European Commission. Glossary and Acronyms (Archived). In Information Society Thematic Portal, http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. Fecha consulta 10.9.2010.

(13) UIT, Rec. UIT-T X.1205. Sector de Normalización de las Telecomunicaciones de la UIT (04/2008). Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. Seguridad en el ciberespacio – Ciberseguridad. Aspectos generales de la ciberseguridad. (04/2008).

zarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y la confidencialidad.»

Implicaciones

Considerando el ciberespacio como un espacio o una colección de recursos, los actores implicados (incluyendo Estados, negocios, organizaciones, grupos o individuos) competirán por controlarlo. Esto conduce inevitablemente a conflictos en el ciberespacio. Se puede definir el ciberconflicto como una confrontación entre dos o más partes, donde al menos una parte utiliza los ciberataques contra el otro. La naturaleza del conflicto diferirá de la naturaleza y objetivos de los participantes. Los delincuentes buscarán ingresos ilegales, de modo que secuestran parte del ciberespacio. Los servicios de inteligencia buscan información útil para atacar a partes enemigas, amistosas o neutrales del ciberespacio para obtener acceso a esa información. Los militares buscan interrumpir las operaciones del enemigo, por ello atacan sistemas de sensores, logísticos, de comunicaciones y control en el ciberespacio enemigo. Los conflictos pueden ser tan simples como disputas civiles sobre la propiedad de un nombre de dominio o más complejos como campañas deliberadas de ciberataques como parte de la guerra convencional entre estados avanzados tecnológicamente.

Dando por supuesto que los ciberconflictos son inevitables, se pueden establecer varias implicaciones desde la variable tiempo de la que depende el ciberespacio. Esta dependencia del tiempo se puede explicar como «el cambio en la estructura y contenido del ciberespacio a lo largo del tiempo». El tiempo en el ciberespacio puede ser relativamente corto: minutos, a menudo incluso segundos o fracciones de segundo. Basándose en esto, se pueden deducir implicaciones como el potencial de los rápidos desarrollos de acciones ofensivas y defensivas, la

viabilidad de trazar el mapa del ciberespacio y la necesidad de patrullarlo y reconocerlo constantemente. Los cambios rápidos en el ciberespacio implican que se necesita poco tiempo para realizar un ataque o para implementar nuevas defensas, comparado con el espacio físico. Un gusano de red que se auto-replica puede infectar enormes partes del ciberespacio en cuestión de minutos. Por ejemplo, en 2003 el gusano SQL Slammer infectó aproximadamente el 90% de los ordenadores vulnerables conectados a Internet en unos 10 minutos de un total de 75.000 máquinas en todo el mundo (14). La única comparación con esto en el espacio físico es el lanzamiento simultáneo de cientos o miles de misiles balísticos armados con cabezas convencionales. Ninguna otra cosa tendría unas consecuencias globales en un intervalo de tiempo similar.

En el lado defensivo, en el ciberespacio es posible mejorar las defensas en segundos o minutos implementando nuevas reglas de cortafuegos, por ejemplo. Construir un nuevo búnker en el espacio físico consume mucho más tiempo. Esto no significa que levantar defensas en el ciberespacio se haga siempre en minutos. Simplemente señala que es posible desplegar medidas defensivas preparadas (reglas más restrictivas de cortafuegos, enrutado y alojamiento alternativo, etc.) en menor tiempo. Al preparar un ciberconflicto es necesario conocer el terreno de la zona potencial de conflicto, las capacidades defensivas y ofensivas de los actores y la posibilidad de daños colaterales y escaladas no planificadas. Por la naturaleza del ciberespacio, es difícil hacer esto, ya que el entorno es complejo y está en constante cambio. Los vectores de entrada potenciales, los objetivos críticos, los usuarios y la información clave pueden cambiar en segundos. Como resultado el mapa sólo puede ser cercano al tiempo real y no hay forma de asegurar que será el mismo el día planificado de ataque (o defensa). Basándose en esto se puede sacar otra implicación. Si el mapa está cambiando constantemente, entonces los esfuerzos de patrulla y reconocimiento deben ser también constantes, de igual manera que se es consciente de la posibilidad de un conflicto en el ciberespacio. Esto significa vigilancia asidua y operaciones con trampa en el lado defensivo e investigaciones habituales en el lado ofensivo. Sin ello, un ataque puede pasar desapercibido o, en el caso ofensivo, el ataque puede frustrarse por un simple cambio en la posición del objetivo. Esta necesidad de actividad constante, sin embargo, eleva

(14) Moore, D. and Paxson, V. and Savage, «*Inside the Slammer Worm*». IEEE Security and Privacy. 2003.

el riesgo de detección por los atacantes y puede delatar los planes y rutinas de los defensores.

Algún autor (15) propone una táctica de defensa proactiva contra estos ataques de las llamadas cibermilicias. Existe una tendencia creciente de cibercampañas que se fijan en los conflictos políticos, económicos o militares en el ciberespacio. El caso de Estonia de 2007 mostró que una nación entera puede verse afectada por ciberataques, mientras que el caso de Georgia de 2008 es un ejemplo de cibercampaña que apunta a un conflicto armado. En ambos casos, al menos parte de los ataques fueron cometidos por hackers patriotas – voluntarios que usan los ciberataques para tomar parte en conflictos internos o internacionales. En estos ciberconflictos comúnmente sólo los objetivos son conocidos mientras que los agresores permanecen en el anonimato. A menudo es difícil averiguar dónde termina la capacidad de un estado y dónde empiezan los grupos de hackers patriotas independientes. Además es relativamente fácil formar una nueva cibermilicia de gente que tiene poca experiencia con ordenadores. El mismo autor define cibermilicia como un grupo de voluntarios que pueden y son capaces de usar los ciberataques para alcanzar un objetivo político. Define cibermilicia on-line como una cibermilicia donde los miembros se comunican principalmente vía Internet y como norma, esconden su identidad. Lo que estos ciberguerreros puedan carecer en formación y recursos, lo suplen con su número. Sin embargo, incluso una cibermilicia ad-hoc que no está bajo control directo de un estado puede ser una extensión útil del poder cibernético de un estado. Por otra parte, ellos también pueden convertirse en una amenaza a la seguridad nacional. Debido a la naturaleza global de Internet, esta amenaza proviene probablemente de múltiples jurisdicciones, lo que limita la aplicación de la ley o las opciones militares del estado. Por tanto, ambos enfoques deberían ser considerados. Para comprender la amenaza potencial de las cibermilicias, sean ad-hoc o permanentes, se necesita explorar cómo están organizadas. A partir de una visión teórica de un tipo concreto de cibermilicia on-line, se proponen tácticas para neutralizarlas. Estas tácticas están basadas en una postura de defensa proactiva y principalmente se usan técnicas de operaciones de información para alcanzar el efecto desde dentro de la propia cibermilicia.

(15) Ottis, Rain, «*Proactive Defense Tactics against on-line cyber militia*». CCD-CoE. Tallinn, Estonia. 2010.

LA SEGURIDAD DEL CIBERESPACIO EN EL ÁMBITO ESPAÑOL

Consideraciones normativas

Una vez vista la importancia de gozar de seguridad en el ciberespacio, cabe la siguiente pregunta: ¿está contemplada la seguridad en el ciberespacio en España?

Aunque España no tiene una estrategia específica sobre Seguridad Nacional y Ciberseguridad, existen desarrollos de otras leyes que abarcan estos aspectos.

En primer lugar en el preámbulo de la Constitución de 1978 se recoge la primera mención a la seguridad: «*La 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*». En su Sección 1ª sobre derechos fundamentales (art. 18) y libertades públicas (art. 20), se recogen aspectos relacionados con la seguridad como son los derechos fundamentales a la intimidad, a la inviolabilidad del domicilio, al secreto de las comunicaciones, limitando el uso de la informática, pero garantizando la libertad de expresión e información.

En el ámbito de la defensa, la *Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional,* menciona los conceptos de seguridad en su exposición de motivos:

«…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 tradicionales para la paz, la estabilidad y la **seguridad**, surgen otros como el terrorismo transnacional con disposición y capacidad de infligir daño indiscriminadamente…«.

La ley define en diferentes Capítulos: las misiones de las Fuerzas Armadas, la contribución a la Defensa, la preparación de recursos para contribuir a la Defensa como son la Guardia Civil, el Centro Nacional de Inteligencia y el Cuerpo Nacional de Policía.

La Directiva de Defensa Nacional 1/2008, y ya anteriormente la de 2004, hace referencia a «un ***sistema de seguridad y defensa español,*** *que debe enmarcarse dentro una* ***Estrategia de Seguridad Nacional».***

Se refiere también a los Principios **de la seguridad y defensa española** y da unas Directrices de carácter general. Esto se traduce en la Directiva de Política de Defensa 1/2009 que es de carácter no público.

Previamente a este desarrollo se habían realizado algunos avances, como lo publicado en el Libro Blanco de la Defensa del año 2000 que definía en su capítulo I, «El Escenario Estratégico», el Panorama de riesgos en 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». En su capítulo III establece la política de defensa española.

Posteriormente, en la Revisión Estratégica de la Defensa del año 2003, en su Planteamiento General establece los intereses nacionales y riesgos para la seguridad. Como otros riesgos para la seguridad considera l*os **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 Fuerzas Armadas, en el sistema nacional de gestión de 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**.»

Ambas experiencias, el Libro Blanco de la Defensa y la Revisión Estratégica de la Defensa de 2003, fueron experiencias aisladas que no tuvieron una continuidad posterior.

Actualmente una comisión de expertos liderados por Javier Solana está elaborando la Estrategia Española de Seguridad que habrá de estar terminada para finales de noviembre. En su elaboración se buscará el mayor consenso político y territorial y la activa participación de la sociedad civil. Esta estrategia tiene en cuenta la cuestión de la ciberseguridad con especial énfasis en la protección de las infraestructuras críticas.

Cómo se gestiona la seguridad en España

A través de la evolución de las TIC han ido surgiendo nuevos riesgos y amenazas, lo que ha implicado la necesidad de gestionar la seguridad de estas tecnologías. En un primer momento, la seguridad se aplicó a la información (Seguridad de la Información) de una manera reactiva, es decir, reaccionando a posteriori una vez surgido el problema de seguridad. En un segundo momento, la evolución ha llevado hacia una postura proactiva (Aseguramiento de la Información) para adelantarse a posibles problemas, esta gestión permite identificar, analizar, gestionar los riesgos y tener previstos planes de contingencia (16).

Como indicaría cualquier metodología de gestión de riesgos, en primer lugar hay que considerar cuáles son los activos del ciberespacio en España. La seguridad y defensa de nuestro ciberespacio comprende, al menos, las infraestructuras críticas, el sector empresarial y la ciudadanía.

Las infraestructuras críticas españolas se agrupan en 12 sectores importantes: administración, agua, alimentación, energía, espacio, industria nuclear, industria química, instalaciones de investigación, salud, sistema financiero y tributario, transporte y tecnologías de la información y las comunicaciones. Todos estos sectores se apoyan en el ciberespacio, tanto para la gestión interna como para la provisión de servicios. Si una

(16) Un ejemplo de gestión de riesgos es la metodología MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, versión 2. El análisis y gestión de los riesgos es un aspecto clave del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. http://www.csae.map.es/csi/pg5m20.htm

contingencia afectara a alguno de los activos de cualquiera de estos 12 sectores estratégicos la seguridad nacional podría verse comprometida.

Respecto al sector empresarial, afortunadamente la mayor parte de las grandes empresas han incorporado la gestión de la seguridad a sus prácticas empresariales. Caso distinto es el de las pequeñas y medianas empresas y autónomos, aunque las TIC han penetrado también en su actividad no se han visto acompañadas por un nivel de seguridad acorde debido a la falta de recursos económicos y humanos.

Los servicios de la sociedad de la información (correo electrónico, comercio electrónico, redes sociales, intercambio de ficheros) están bastante asimilados en la ciudadanía que se encuentra con el posible compromiso de sus libertades y derechos individuales por parte de cualquiera de los tipos de amenazas existentes en el ciberespacio.

Al igual que en países de nuestro entorno, la legislación en España se está adaptando a los nuevos retos y amenazas provenientes del ciberespacio, tanto con medidas preventivas como reactivas (17). En el primer caso, se sitúa la siguiente normativa:

- Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)
- Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAESCSP)
- Real Decreto RD 1671/2009 por el que se desarrolla parcialmente la LAESCP
- Real Decreto 3/2010 en el que se aprueba el Esquema Nacional de Seguridad
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD)
- Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la LOPD
- Ley 59/2003 de Firma Electrónica

En concreto, el Esquema Nacional de Seguridad establece la política de seguridad en la utilización de medios electrónicos por las administraciones públicas y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Este RD dedica todo su Capítulo VII a la Capacidad de Respuesta a Incidentes de Seguridad, CCN-CERT, del Centro Criptológico Nacio-

(17) Informe de Amenazas CCN-CERT IA-03/10. Ciberamenazas 2009 y tendencias 2010.

nal (CCN), adscrito al Centro Nacional de Inteligencia (CNI). Así, en su artículo 36, el real decreto señala que el CCN «articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN».

En la modificación de la Ley del Código Penal de 1995 (18) se han incluido los ataques informáticos, entre las medidas sancionadoras destacan como conductas punibles las consistentes en:

- Borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos.
- Obstaculizar o interrumpir el funcionamiento de un sistema de información ajeno.
- El acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema informático o en parte del mismo.

En esta reforma también se incluyen otros nuevos delitos, como la captación de menores para espectáculos pornográficos o el tráfico ilegal de órganos. También se contemplan nuevas penas o la responsabilidad penal de las personas jurídicas. Los delitos relacionados con la propiedad intelectual también han sido modificados, de manera que se reduce la pena de cárcel a multa o a trabajos en beneficio de la comunidad cuando la venta de material audiovisual, el conocido como top manta, sea al por menor y el beneficio económico sea bajo.

Otra iniciativa de finales de 2009, fue la firma de un convenio para la conexión informática de todos los órganos judiciales, entre el ministro de Justicia, el presidente del Consejo General del Poder Judicial, el fiscal general del Estado y las 11 Comunidades Autónomas con competencias en la materia. A través del proyecto EJIS (Esquema Judicial de Interoperabilidad y Seguridad) todas las unidades judiciales del país podrán trabajar en red y conocer en tiempo real la información que sobre un determinado asunto o persona se tiene en otro juzgado.

---

(18) Modificación del Código Penal que establece penas de prisión para el acceso no autorizado y el daño a sistemas informáticos. 23 de junio de 2010, BOE con Ley Orgánica 5/2010 de 22 de junio que modifica la LO 10/1995 de 23 de noviembre del Código Penal que entrará en vigor el 23 de diciembre.

Como se ha mencionado anteriormente, la seguridad de las infraestructuras críticas es un aspecto estratégico para garantizar la propia seguridad de nuestros países y nuestros ciudadanos. Cualquier estrategia de seguridad nacional 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.

Respecto a las infraestructuras críticas, en 2007, se creó dependiente del Ministerio del Interior el CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) con el cometido 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; fomentar las buenas prácticas; y establecer contactos y mecanismos de colaboración con centros similares en todo el mundo.

Durante el año 2008, el CCN-CERT inició el despliegue de un sistema de alerta temprana en la Red SARA (puesta a disposición de todas las administraciones públicas), con el fin de detectar de manera proactiva las anomalías y ataques del tráfico que circula entre los diferentes ministerios y organismos conectados.

A las iniciativas de Centros de Respuesta a Incidentes existentes ya en 2008, el año 2009 ha visto el desarrollo de diversas iniciativas en el marco de las comunidades autónomas. Así, al CSIRT-CV (de la Comunidad Valenciana, se ha venido a sumar el Centro de Seguridad de la Información de Catalunya (CESICAT) y el Centro de Seguridad TIC de Andalucía.

Además INTECO (Instituto Nacional de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, Turismo y Comercio, es responsable de gestionar a través de su CERT la defensa del ciberespacio relacionado con las PYMES españolas y los ciudadanos en su ámbito doméstico. Anualmente desde 2007 organiza ENISE, Encuentro Internacional de la Seguridad de la Información (19) que pretende convertirse en un gran encuentro de los principales agentes en el campo de la seguridad (industria, I+D, administraciones públicas, usuarios, etc.), tanto de la UE como de Iberoamérica.

El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la

(19) Consúltese http://www.inteco.es/ y http://enise.inteco.es

Policía Nacional, dependientes ambos del Ministerio del Interior son responsables de combatir la delincuencia que se produce en el ciberespacio.

La Agencia Española de Protección de Datos (AGPD) (20), dependiente del Ministerio de Justicia, es responsable de hacer cumplir la normativa en materia de protección de datos personales, junto con las agencias autonómicas (Madrid, Cataluña y País Vasco) (21).

Por otra parte, en el ámbito de normalización, AENOR, Asociación Española de Normalización y Certificación, colabora al menos, con dos subcomités técnicos (22), el AEN/CTN 71/SC27 sobre Técnicas de seguridad de las Tecnologías de la información y el AEN/CTN 196/ SC1 sobre Continuidad de infraestructuras y servicios críticos relativo a la Protección y seguridad de los ciudadanos, que tienen en consideración la directrices europeas (23).

Entre los estándares aprobados destaca la serie ISO/IEC 27000 sobre Sistemas de Gestión de Seguridad de la Información (SGSI), con definición de vocabulario, fundamentos, requisitos, guía de buenas prácticas, etc. (24).

---

(20) La AEPD destaca en su Memoria 2009 el incremento en más del 75% del número de denuncias recibidas, que evidencia que los ciudadanos cada vez son más conscientes de su derecho a la protección de datos, así como de la existencia de una institución encargada de protegerlos. Los sectores que más sanciones acumulan son los de telecomunicaciones, videovigilancia y sector financiero. Consúltese en http://www.agpd.es

(21) Protección de Datos abre un procedimiento sancionador contra Google. El trámite se paraliza a la espera de que un juzgado de Madrid resuelva sobre la captación de datos de redes wifi privadas accesibles desde las calles por donde circulaban los coches de su callejero virtual Street View. La apertura del procedimiento sancionador se produce tras constatar la existencia de indicios de la comisión de dos infracciones graves y tres muy graves de la ley de protección de datos, como la captación y almacenamiento de datos personales sin consentimiento. Enlace: www.elpais.com. Fecha consulta 19.10.2010.

(22) http://www.aenor.es/aenor/normas/ecomites/ecomites.asp

(23) Dictamen del Comité Económico y Social Europeo sobre la «Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia»» C 255/98, de 22.9.2010.

(24) Desde AENOR y sus grupos de expertos se estudian los riesgos en las TICs y su solución: la posible aplicación de normas internacionales ISO y otras normas. Se estudian las TICs y su integración en el Negocio, considerando los siguientes aspectos con su norma de aplicación respectiva:
- Riesgos en IT Governance. Gobierno de TI. ISO 38500;
- Riesgos en el Desarrollo del Software. ISO-SPICE 15504;
- Riesgos en los servicios de TI. ISO -20000-1;
- Riesgos en la Seguridad de los Sistemas de Información. ISO 27001;
- Riesgos en la Continuidad del Negocio. BS25999.

Hay que destacar también que, de acuerdo al Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) (25), ámbito de actuación del Centro Criptológico Nacional, se pueden certificar aquellos sistemas y productos que cumplen con los criterios, métodos y normas de evaluación de la seguridad, como la normativa europea conocida como ITSEC (26) y la normativa internacional conocida como Criterios Comunes (27).

Otra iniciativa del Ministerio de Defensa, presentada recientemente, es la Estrategia de Tecnología e Innovación para la Defensa, ETID-2010 (28) con objeto de cumplir con una de las directrices de la Directiva de Defensa Nacional 1/2008 que establece la necesidad de fomentar la investigación, desarrollo e innovación para mantener un nivel tecnológico elevado que sea capaz de apoyar las necesidades de la seguridad y poder integrarse en el esfuerzo europeo. De aquí puede derivarse una posible propuesta para la Estrategia Española de Seguridad, considerando que, la innovación tecnológica debería contemplarse como un factor determinante en la seguridad de España, donde su tejido empresarial y tecnológico puede y debe jugar un papel fundamental y en la que el esfuerzo en innovación serán los elementos claves.

Dentro de las iniciativas del Ministerio de Industria, Turismo y Comercio, el Plan Avanza2, dado a conocer en julio pasado para su estrategia 2011-2015, se ha estructurado en torno a cinco ejes de actuación concretos entre los que están presentes las infraestructuras críticas y el refuerzo policial en delitos informáticos (29).

---

(25) Véase http://www.oc.ccn.cni.es

(26) Véase ITSEC/ITSEM en http://www.oc.ccn.cni.es/normas_es.html

(27) Common Criteria http://www.commoncriteriaportal.org

(28) *Estrategia de Tecnología e Innovación para la Defensa, ETID-2010*. Ministerio de Defensa. Dirección General de Armamento y Material. Subdirección General de Tecnología y Centros. Enlace: http://www.mde.es/Galerias/politica/armamento-material/ficheros/DGM_ETID_v5d.pdf

(29) http://www.planavanza.es Los cinco ejes del Plan Avanza2 son: Infraestructuras; Confianza y Seguridad; Capacitación tecnológica; Contenidos y Servicios Digitales; y Desarrollo del sector TIC. Incluye la definición de más de 100 medidas concretas. Respecto al apartado «Confianza y Seguridad», el Plan Avanza2 identifica cuatro aspectos: extender la cultura de la seguridad a la ciudadanía y las PYMES; gestionar la privacidad de forma equilibrada; generalizar el uso del dni electrónico, así como de la identidad y firma digital; y responder proactivamente a los incidentes de seguridad. Para ello, se desarrollarán campañas e iniciativas de concienciación así como de colaboración entre organismos nacionales y europeos. En este último apartado se recogen las medidas más significativas: mayor protección de las infraestructuras críticas;

EL ÁMBITO EUROPEO, DE LA OTAN Y EL NORTEAMERICANO

La Unión Europea

La UE aprobó en diciembre de 2002 la Estrategia Europea de Seguridad (EES) donde se planteaba una Europa segura en un mundo mejor. En ella consideraba el contexto de seguridad con los desafíos mundiales y principales amenazas (30). Ese contexto de seguridad producto del fin de la guerra fría, se caracteriza por una apertura cada vez mayor de las fronteras que vincula indisolublemente los aspectos internos y externos de la seguridad. Ha habido un desarrollo tecnológico que ha incrementado el grado de dependencia de Europa respecto de una infraestructura interconectada en ámbitos como el transporte, la energía o la **información**, aumentando por ende su vulnerabilidad.

En la Revisión de la EES, el llamado Informe Solana**,** de diciembre de 2008 ya aparece dentro de las nuevas amenazas y riesgos, la **seguridad de los sistemas de información**. Como uno de los nuevos retos mundiales y principales amenazas menciona el concepto de **Ciberseguridad:** «Las economías modernas dependen en gran medida de las infraestructuras vitales como los transportes, las comunicaciones y el suministro de energía, e igualmente de **internet.** La Estrategia de la UE para una **sociedad de la información segura** en Europa, adoptada en 2006, hace referencia a la delincuencia basada en internet. Sin embargo, los ataques contra sistemas de TI privadas o gubernamentales en los Estados miembros de la UE han dado una nueva dimensión a este problema, en calidad de posible nueva arma económica, política y militar. Se debe seguir trabajando en este campo para estudiar un planteamiento general de la UE, concienciar a las personas e intensificar la cooperación internacional.»

En marzo de este año además, se ha aprobado la Estrategia de Seguridad Interior de la UE (31), que se extiende también a múltiples sectores

---

esfuerzo de los servicios policiales especializados en delitos informáticos; impulso de las medidas definidas en el Esquema Nacional de Seguridad; cooperación mutua entre los organismos nacionales de respuesta; reforzamiento de las principales líneas de actuación de INTECO, su CERT, el Observatorio de la Seguridad de la Información y la Oficina de Seguridad del Internauta. Se plantea también, el impulso en el marco de la UE de un Plan Europeo de Ciberseguridad en la red.

(30) Estrategia Europea de Seguridad (EES) 2003. http://www.ieee.es/Galerias/fichero/estrategia_europea_de_seguridad_2003.pdf. Fecha consulta 13.9.2010.

(31) Estrategia de Seguridad Interior de la UE. Enlace: http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf

para hacer frente a amenazas graves. Entre las amenazas que define esta estrategia se incluye la ciberdelincuencia.

Europa, con su Política de Seguridad y Defensa Común (1999), ha desarrollado, programas y estructuras de defensa para protegerse como órgano unitario, y a cada uno de sus miembros, contra los riesgos y amenazas. Como iniciativas más importantes sobre seguridad se subrayan:

- Creación de ENISA (Agencia Europea de Seguridad de las Redes y de la Información) en 2004, otorga asesoramiento a la Comisión y los estados miembros en lo relacionado a seguridad y productos informáticos (32).
- Programa para la Protección de la Infraestructuras Críticas (PEPIC), aprobado en 2004.
- Proteger Europa de ciberataques e interrupciones a gran escala aumentar la preparación, seguridad y resistencia (33).
- Hacia una política general de lucha contra la delincuencia (34).
- Agenda Digital Europea (35): estructura sus acciones clave, en torno a la necesidad de abordar sistemáticamente los siete aspectos problemáticos que se enumeran a continuación: 1) Fragmentación de los mercados digitales; 2) Falta de interoperabilidad; 3) Incremento de la **ciberdelincuencia** y riesgo de escasa confianza en las redes; 4) Ausencia de inversión en redes; 5) Insuficiencia de los esfuerzos de investigación e innovación; 6) Carencias en la alfabetización y la capacitación digitales; 7) Pérdida de oportunidades para afrontar los retos sociales.

Esta Agenda constituye una instantánea de los problemas y oportunidades actuales y previsibles, y evolucionará a la luz de la experiencia y de las rápidas transformaciones de la tecnología y la sociedad. Por otro lado se plantean un conjunto de iniciativas legislativas propuestas en

(32) Dictamen del CES Europeo sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones», C255/98. 22.9.2010. Comunicación COM(2009) 149 final, 30.3.2009.

(33) Dictamen del CES Europeo sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones», C255/98. 22.9.2010. Comunicación COM(2009) 149 final, 30.3.2009.

(34) Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones», COM (2007) 267 final.

(35) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una Agenda Digital para Europa. Enlace: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:ES:PDF, mayo de 2010. Fecha consulta 23.9.2010.

el marco de esta Agenda Digital, distribuidas en los siguientes puntos: a) Un mercado único digital dinámico; b) Interoperabilidad y normas; c) Confianza y **seguridad;** d) Acceso rápido y ultrarrápido a Internet; e) Fomentar la alfabetización, la capacitación y la inclusión digitales; f) Beneficios que hacen posibles las TIC para la sociedad de la UE.

Son muchos los pasos dados en el marco europeo pero hace falta más. En el núcleo del desarrollo de una política de ciberseguridad europea se encontraría el desarrollo de una Estrategia Europea de Ciberseguridad. Así lo indicó el director ejecutivo de ENISA, en una conferencia impartida en Madrid sobre protección de infraestructuras críticas afirmando que Europa necesita una estrategia integral de ciberseguridad que integre a las diferentes estrategias nacionales. El Parlamento Europeo recogió esta propuesta en una resolución sobre la aplicación de la Estrategia Europea de Seguridad y la Política Común de Seguridad y Defensa. Otras propuestas incluyen la creación de un consejo, de un coordinador o de una agencia de ciberseguridad europea.

El marco OTAN

La Revisión del Concepto Estratégico de 1999 también considera la **ciberseguridad** como un nuevo reto respecto al concepto estratégico de 1999. La OTAN está evolucionando. Está cambiando. Se estima que a finales de 2010 aparecerá el Nuevo Concepto Estratégico (NCEO) pues el actual ya no se considera viable. En la guerra asimétrica del siglo XXI, la OTAN necesita actualizarse tecnológicamente. En cuestiones de guerra electrónica, OTAN está desplegando su política de ciberdefensa (36). La creación del concepto de ciberdefensa y la inauguración del Centro de Excelencia en Ciberdefensa en Tallinn, Estonia es un ejemplo de ello. En el nuevo concepto se tendrán en cuenta la política de ciberdefensa y la política de guerra electrónica.

USA

Con la llegada del presidente Obama se han potenciado las iniciativas en ciberseguridad. La administración Obama ha publicado una iniciativa de ciberseguridad (37).

---

(36) Marios PANAGIOTIS, «*Challenging NATO's Security Operations in Electronic Warfare: The policy of Cyber-Defence*». 2009.

(37) The Comprehensive National Cybersecurity Initiative. 2009. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf. Fecha consulta 23.9.2010.

A partir de los ataques del 11 de septiembre de 2001, Estados Unidos cambió su Estrategia de Seguridad centrándola en los siguientes pilares:

- El establecimiento y reordenación de las responsabilidades relativas a la seguridad del territorio (entre las cuales se encuentran también las relacionadas con la ciberdefensa).
- El desarrollo de legislación relativa a la Seguridad Nacional y la ciberdefensa.
- El desarrollo de planes y estrategias relativas a la Seguridad Nacional:
  - Seguridad del territorio.
  - Seguridad del ciberespacio.
  - Ejecución de ejercicios periódicos de ciberseguridad (38).
  - Seminarios periódicos sobre concienciación en la ciberseguridad.
  - Plan Nacional de Protección de Infraestructuras.

Del conjunto de estrategias, se fijan cinco prioridades nacionales en esta materia:

- Sistema de Respuesta Nacional de la Seguridad en el Ciberespacio (39).

---

(38) El ejercicio 'Cyber Storm III', involucra a empleados de siete departamentos del Gobierno de EEUU, incluido el Pentágono, once estados federados, 60 empresas privadas y 12 socios internacionales. Organizado por el Departamento de Seguridad Nacional, representa la primera oportunidad de probar el nuevo centro nacional para la integración de la seguridad cibernética, inaugurado en octubre de 2009, que coordina a los expertos de los sectores público y privado. http://www.elmundo.es/elmundo/2010/09/28/navegante. Fecha consulta 29.9.2010.

(39) Controvertidas iniciativas del Gobierno de los Estados Unidos para subsanar sus deficiencias en materia de «ciberseguridad». Según el informe entregado por el inspector general del Departamento de Seguridad Nacional de EEUU al Comité de Seguridad Nacional, con los principales hallazgos de una inspección independiente, demuestra que el US-CERT (United States-Computer Emergency Readiness Team) no está cumpliendo su función con eficacia. El US-CERT se creó en 2003 para encargarse de analizar y reducir las ciberamenazas y vulnerabilidades, difundir información sobre alertas de amenazas de seguridad, y coordinar las actividades de respuesta antes incidentes cibernéticos. El informe pone de manifiesto falta de personal y no compartir información suficiente sobre amenazas y vulnerabilidades. Los responsables de elaborar las leyes federales norteamericanas están considerando modificar la legislación para redefinir el papel del Gobierno en materia de «ciberseguridad». Entre esos proyectos legislativos se halla la propuesta legislativa «Protecting Cyberspace as a National Asset Act of 2010» que pretende coordinar los elementos clave que se necesitan para proteger las infraestructuras críticas norteamericanas, centrándose en la capacidad de alerta temprana, los procesos continuos de monitorización en tiempo real y en la modernización de la «Ley de Gestión de la Seguridad de la Infor-

- Programa de Reducción de Amenazas y Vulnerabilidades para la Seguridad del Ciberespacio.
- Programa de Formación y Concienciación de la Seguridad en el Ciberespacio.
- Asegurar el ciberespacio gubernamental.
- Cooperación nacional e internacional para la Seguridad en el Ciberespacio.

TIPOS ATAQUES Y ATACANTES

Tipos de ataques

La literatura existente sobre los tipos de ataques es muy amplia. Los ataques surgen al mismo tiempo que las tecnologías de la información, en estas tecnologías no sólo se engloban los ordenadores sino cualquier dispositivo electrónico, como es el caso de los teléfonos móviles, las agendas electrónicas, GPS, las tabletas electrónicas, etc., así como las comunicaciones. Estos ataques pueden afectar a cualquier nivel: ciudadanos, empresas, administración, infraestructuras críticas, sector bancario, etc. Se habla incluso de amenazas avanzadas (40).

La mayoría de los ataques se aprovechan de vulnerabilidades de los sistemas informáticos, agujeros de seguridad que surgen de una deficiente programación que no tiene en cuenta la seguridad en el ciclo de vida del desarrollo del software y los diversos protocolos de comunicación.

Con el tiempo muchos protocolos fueron avanzando hacia versiones más seguras, por ejemplo Telnet y SSL, http y https, ftp y sftp, etc.

---

mación Federal» FISMA. Este proyecto también plantea la creación de dos oficinas: una oficina de ciberseguridad dentro de la Casa Blanca que le asesoraría en materia de ciberseguridad, supervisaría todas las actividades del ciberespacio, y se encargaría de desarrollar una estrategia de ciberseguridad nacional; y otra oficina dentro del Departamento de Seguridad Nacional, Centro Nacional de Ciberseguridad y Comunicaciones (NCCC) que se encargaría de encabezar los esfuerzos federales de cara a la protección de las redes públicas y privadas, exigir el cumplimiento de las políticas de ciberseguridad tanto en el gobierno como en el ámbito civil.

(40) Aunque las «amenazas avanzadas» cada vez son más numerosas y difíciles de detectar, las organizaciones carecen de medios, tecnología y personal para abordarlas. Este es el principal hallazgo del estudio «Growing Risk of Advanced Threats» realizado por el Instituto Ponemon, para cuya elaboración encuestó a 591 trabajadores del ámbito de las TI y de la seguridad TI, asentados en los EEUU. Este informe define «amenaza avanzada» como «una metodología empleada para evadir las medidas de protección de una compañía, con el fin de desencadenar una variedad de ataques con un objetivo concreto».

Un caso especial son las redes sociales cuya falta de seguridad afecta a la ciudadanía, en especial, a los menores, que en ocasiones son objeto de la llamada ingeniería social y acaban siendo víctimas de acoso sexual, o revelación de información personal.

Algunos de los tipos de ataques más conocidos y cuya definición figura en una de las guías del CCN-CERT (41) son:

- Virus**:** Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
- Código dañino, también conocido como código malicioso, maligno o «malware» en su acepción inglesa: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial (42).
- Bomba lógica: Segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica (por ejemplo, número de accesos a una parte del disco) o temporal (satisfacción de una cierta fecha). Cuando ello ocurre desencadenen a alguna acción no autorizada. En ocasiones, si la condición a verificar es una cierta fecha, la bomba se denomina temporal.
- Troyano: Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.
- Gusano: Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

Tipos de atacantes

Los atacantes se pueden clasificar atendiendo a su motivación: como puede ser la búsqueda de un cambio social o político, un beneficio económico, político o militar, o satisfacer el propio ego; su objetivo: ya sean

(41) Guía de seguridad de la STIC (CCN-STIC-401), Glosario y abreviaturas, 1 de febrero de 2010.

(42) En el informe de inteligencia de seguridad aparece España entre los países con más infecciones por malware del mundo detrás de Corea del Sur con 12,4 infecciones por cada 1.000 computadoras escaneadas). Battling botnets for control of computers. SIR -Microsoft Security Intelligence Report, volume 9, January through June 2010.

individuos, empresas, gobiernos, infraestructuras, sistemas y datos de tecnologías de la información, ya sean públicos o privados; el método empleado: código dañino, virus, gusanos, troyanos, etc.

Atendiendo a su autoría se pueden clasificar en:

- **Ataques patrocinados por Estados:** los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. En los últimos años se han detectado ciber-ataques contra las infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. El ejemplo más conocido es el ataque a parte del ciberespacio de Estonia en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico o los ciber-ataques sufridos por las redes clasificadas del gobierno estadounidense a manos de atacantes con base en territorio chino o el último ataque reconocido por Irán a los sistemas informáticos de decenas de industrias que fueron atacados por un virus antes de este verano (43) y del que Irán dice haberse recuperado (44). Aquí también puede incluirse el espionaje industrial.
- **Servicios de inteligencia y contrainteligencia**: empleados por los estados para realizar operación de información. Suelen disponer de bastantes medios tecnológicos y avanzados.
- **Terrorismo, extremismo político e ideológico:** los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas, así como herramienta de financiación. Estos grupos ya han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses.
- **Ataques de delincuencia organizada:** las bandas de delincuencia organizada han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. Este tipo de bandas tienen como objetivo la obtención de información sensible para su posterior uso fraudulento y conseguir grandes beneficios económicos (45).

---

(43) El Mundo: Irán reconoce un ataque informático masivo por el gusano Stuxnet contra sus sistemas industriales. Artículo publicado en la edición digital del diario El Mundo. Enlace http://www.elmundo.es/elmundo/2010/09/27/navegante/1285571297.html. Fecha consulta 27.9.2010.

(44) Revista Atenea: Irán dice haber limpiado todos los ordenadores infectados por virus Stuxnet. http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_3060_ESP.asp. Fecha consulta 4.10.2010.

(45) Según datos del FBI, en 2009 el impacto de la ciberdelincuencia por la acción de bandas organizadas ocasionó unas pérdidas, tanto a empresas como a particulares

- **Ataques de perfil bajo.** Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos TIC que les permiten llevar a cabo ciberataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal.

Evolución de los ciberataques

Las vulnerabilidades de los sistemas son el elemento fundamental de los ciberataques porque es la esencia de las capacidades ofensiva, defensiva y de inteligencia en el ciberespacio (46). Es importante mirarlo desde el punto de vista de estas tres capacidades. A menudo se trata como una exposición y un riesgo. Este es el punto de vista de la ciberdefensa. Estas vulnerabilidades son el modo de crear ciberarmas y de infiltrarse en sistemas para recoger inteligencia. Las ciberarmas viajan a la velocidad de la luz, pueden lanzarse desde cualquier lugar del mundo y alcanzan el blanco en cualquier lugar. Los ordenadores, sistemas y redes con vulnerabilidades expuestas pueden ser interrumpidos o tomados por un hacker o por un código dañino automático. Algunos líderes militares ven las ciberarmas como armas de destrucción masiva. De hecho, se ha creado un nuevo término en relación a los ciberataques, armas de interrupción masiva.

Ha habido una evolución en el diseño de las llamadas ciberarmas. Al principio de los años 80 del pasado siglo comenzó el código dañino. Desde entonces, aumentó la frecuencia de este tipo de código así como la naturaleza destructiva y su calidad. A mediados de los 90 ya había virus, gusanos, troyanos y código especialmente diseñado y desarrollado para robar información de los ordenadores. A comienzos de 2000 la delincuencia organizada ya se había percatado del valor y el beneficio de desarrollar y usar código dañino como parte de su negocio ilegal. Las ciberarmas son programas que atacan uno o varios objetivos. Muchos de estos programas están disponibles en Internet de forma gratuita o a un coste relativamente bajo, sin embargo, las armas más sofisticadas no están disponibles o están a la venta en sitios web piratas.

En esta evolución hubo un punto de inflexión en el período 2003-2004 en el que se produjo un cambio sustancial: los desarrolladores de código dañino se profesionalizaron, usaban ya metodologías formales para desarrollar código. No escribían código simplemente, sino que

---

estadounidenses, por un valor superior a 560 millones de dólares.

(46) Kevil Coleman, «*The weaponry and strategies of digital conflict*». Security and Intelligence Center at the Technolytics Institute, USA, 2010.

desarrollaban código mediante un proceso de garantía de calidad para mejorar su funcionamiento y fiabilidad. Actualmente se está observando otro avance significativo en el desarrollo de código dañino utilizado como ciberarma: la arquitectura modular.

A principios de este año, el jefe de ciberseguridad de la OTAN avisaba que los ciberataques y el ciberterrorismo suponen la misma amenaza para la seguridad nacional que un misil. Si por ejemplo determinado misil intercontinental tiene un alcance de unos 12.000 km y viaja a 24.000 km/hora, un ciberarma tiene un alcance ilimitado y viaja a casi la velocidad de la luz a 297.000 km/s. Mediante la comparación con un misil, se pone en contexto la arquitectura evolucionada de las ciberarmas. Un misil está compuesto por tres elementos básicos: el primero es el motor o planta propulsora, seguido por un sistema de guiado (que indica cuál es el objetivo) y finalmente la carga útil (el componente que causa el daño). Veamos cómo los mismos tres elementos aparecen en el diseño de un ciberarma.

El motor: existen numerosos métodos para que un ciberarma alcance sus objetivos. Un ejemplo de métodos de entrega son los correos electrónicos con código dañino incluido o anexado, sitios web con enlaces o descargas infectadas, el llamado hacking es el método empleado por un atacante para colocar una carga maliciosa en un ordenador, sistema o red. La falsificación de elementos hardware, software o componentes electrónicos son también otros métodos utilizados.

El sistema de guiado: de igual manera que guía un misil, el componente de guiado de un ciberarma permite que la carga útil alcance un punto concreto dentro del ordenador, sistema o red aprovechando una vulnerabilidad concreta. Las vulnerabilidades de sistema son el objetivo principal de estos sistemas de guiado. Las vulnerabilidades en el código y en la configuración de los sistemas informáticos proporcionan puntos de entrada para la carga dañina. Las brechas de seguridad de los sistemas operativos, aplicaciones, código, también a nivel de microprocesador, permiten la explotación no autorizada. La explotación de estas vulnerabilidades puede permitir un acceso remoto no autorizado y controlar el sistema. Es importante destacar que en 2007 se informó como media de una nueva vulnerabilidad cada 57 minutos.

La carga útil: la carga útil de un misil se denomina cabeza y se empaqueta con algún tipo de explosivo; en un ciberarma la carga útil puede ser un programa que copia información del ordenador y la envía a un destino externo. También puede ser un programa que borra o altera la

información almacenada en el sistema. Incluso puede permitir acceso remoto al ordenador de modo que puede controlarse desde la red. Las bot (de botnets) (47) son un ejemplo de una carga útil que permite el uso remoto de un ordenador por un usuario u organización no autorizada.

Estos tres elementos muestran el avance y la sofisticación que han alcanzado las ciberataques. Esta arquitectura emplea la reutilización de los tres componentes. Así, si se descubre una determinada vulnerabilidad, se informa de ello y se instala el parche de seguridad relativo a esa vulnerabilidad de código, entonces ese componente de la ciberarma se puede quitar y sustituir, mientras que los otros dos componentes aún son útiles. Esto no sólo crea flexibilidad sino que incrementa significativamente la productividad de los desarrolladores de las ciberarmas. Las capacidades de desarrollo de ciberarmas es una competencia crucial para alcanzar la seguridad nacional. Hemos entrado en una nueva carrera armamentística –la carrera ciberarmamentística–. Un informe de la compañía RAND mostró que el coste de desarrollo de ciberarmas para emprender una ciberguerra es extremadamente modesto. Esto pone esta nueva clase de armas al alcance de cualquier país y organización terrorista. Además estas armas se diseñan y desarrollan de forma profesional y existen traficantes de ciberarmas. Un reciente informe afirmaba que el 90% de los sitios web examinados con código dañino residían en servidores localizados en USA o Reino Unido. En el mismo informe, oficiales de contrainteligencia de USA afirmaban que unas 140 organizaciones de inteligencia extranjeras intentaban regularmente atacar ordenadores, sistemas y redes de las agencias del gobierno USA. Además, ordenadores pertenecientes a Al Qaeda y otras organizaciones que habían sido confiscadas legalmente indican que los miembros de grupos terroristas, cada vez están más familiarizados con herramientas y servicios de ataque (hacking) que están disponibles en la red.

La amenaza a las Infraestructuras Críticas

Las amenazas enemigas de las infraestructuras críticas (IC) siempre han existido en tiempos de guerra o conflicto, pero los escenarios de amenazas incluyen ahora ataques en tiempos de paz por ciberatacantes anónimos (48). Los sucesos actuales, incluyendo los ejemplos de Israel

(47) Botnet (ro**bot net**work): término que hace referencia a un conjunto de *robots informáticos* o *bots*, que se ejecutan de manera autónoma y automática y que puede controlar todos los ordenadores/servidores infectados de forma remota. Fuente: Wikipedia.

(48) Geers, Kenneth, «*The Cyber Threat to National Critical Infrastructures: Beyond theory*«. Information Security Journal: A global perspective, 18:1-7, 2009.

y Estonia, demuestran que se puede alcanzar cierto nivel de disturbio real sólo con paquetes de datos hostiles. Los logros asombrosos de la ciberdelincuencia y el ciberespionaje, contra los que la ley y la contrainteligencia han encontrado poca respuesta, indican que es sólo cuestión de tiempo enfrentarse a ciberataques serios contra las IC. Es más, los estrategas de la seguridad nacional deberían tratar todas las amenazas con método y objetividad. A medida que crece la dependencia de las tecnologías de la información (TI) y de Internet, los gobiernos deberían invertir proporcionalmente en seguridad de redes, respuesta a incidentes, formación técnica y colaboración internacional.

El ciberespacio está cambiando nuestra vida tal como la conocemos, para incluir la naturaleza y comportamiento de la ciberguerra. Mientras que las amenazas a las IC han existido siempre durante tiempos de guerra, las amenazas ahora incluyen ataques en tiempos de paz, por atacantes que pueden permanecer completamente anónimos. Los sucesos actuales muestran que la cuestión ya no es si los ciberatacantes cogerán por sorpresa a los estrategas de la seguridad nacional, sino cuándo y bajo qué circunstancias. Los casos de Israel y Estonia demuestran que se puede lograr un cierto grado de desorden real sólo con unos paquetes de datos: los bancos se quedaron sin conexión, los medios de comunicación se silenciaron, se bloqueó el comercio digital y se amenazó la conectividad gubernamental junto a sus ciudadanos. Véase también el último caso padecido por Irán durante el verano (49). Hasta cierto punto todas las IC son vulnerables, pero la vulnerabilidad real, especialmente ante un ciberataque, es teórica por naturaleza. En su debido momento, conforme el mundo real y el virtual interactúan mutuamente desde una base más cercana, los ataques futuros acercarán la teoría y la realidad. Mientras las naciones fuertes en TI tienen numerosas ventajas sobre otros países menos conectados, el ciberespacio es un medio prodigioso mediante el que una parte más débil puede atacar a un contrincante más fuerte convencionalmente. Actualmente, como los ciberatacantes parecen contar con ventaja, muchos gobiernos y actores no estatales probablemente han llegado a la conclusión de que la mejor ciberdefensa es un buen ataque. Las victorias tácticas, incluso de naturaleza digital únicamente, pueden afectar al proceso de toma de

(49) El País. «Alarma por un virus pensado para el sabotaje industrial y la ciberguerra». Stuxnet ataca un programa de gestión de centrales eléctricas, oleoductos y conglomerados fabriles.- Irán admite ser víctima del mismo. Enlace: http://www.elpais.com/articulo/tecnologia/Alarma/virus/pensado/sabotaje/industrial/ciberguerra. Fecha consulta 27.9.2010.

decisiones a nivel estratégico, especialmente si ellos amenazan las IC del enemigo. Por tanto, es primordial que la defensa ante operaciones hostiles en red –desde propaganda, espionaje a ataques a IC– deba jugar un papel en todos los planeamientos de seguridad nacional. Es más, los estrategas de seguridad nacional deberían permanecer equilibrados y tratar las ciberamenazas con método y objetividad. Primero, deberían evaluar el nivel de dependencia de sus IC respecto de las TI y, en segundo lugar, el nivel de conectividad al ciberespacio. Finalmente, deberían imaginar vívidamente los peores escenarios: si un actor hostil tuviera el control completo de un sistema crítico ¿cuánto daño podría causar?. Merece la pena considerar que intentar un ciberataque puede ser más fácil y barato que montar un ataque físico, aunque el nivel y duración de la interrupción que un ciberataque produzca sea proporcionadamente menor (50). Para un futuro predecible, infligir un daño duradero sobre IC sólo mediante ciberataques es muy poco probable. Las ICs se diseñaron para poder fallar y ser reiniciadas. Por tanto, el objetivo no debería ser la perfección, sino una buena gestión de crisis. Con el tiempo, conforme el control de las IC se desplaza desde redes dedicadas a Internet, y se emplean protocolos de red comunes sobre los propietarios, aumentarán las oportunidades de que los atacantes invadan los sistemas cerrados. A medida que crece nuestra dependencia de las TI y la conexión al ciberespacio, los gobiernos deberían hacer mayores inversiones en seguridad de redes, respuesta a incidentes y formación técnica para el cumplimiento de la ley. Finalmente, deberían invertir en iniciativas de colaboración internacional específicamente diseñadas para contrarrestar la naturaleza transnacional de los ciberataques.

NECESIDAD DE ESTRATEGIAS DE CIBERSEGURIDAD

Los militares alrededor del mundo están ocupados diseñando estrategias contra la ciberguerra y la doctrina operacional que necesitan en este entorno único de amenazas. No es una tarea pequeña dadas las características de las ciberoperaciones ofensivas y defensivas y del análisis y recopilación de ciberinteligencia. El anterior Secretario de Estado de Interior estadounidense afirmó que la comunidad internacional debe escribir la doctrina de ciberguerra y pregunta ¿cuál es el significado de la disuasión en un mundo de ciberguerra? Estas afirmaciones deben recibir una respuesta pronto. Sin embargo, la necesidad de doctrina y estrategias no se termina aquí.

(50) Lewis, J. A., «*Assessing the risks of cyber terrorism, cyber war and other cyber threats*», Center for Strategic and International Studies. (2002 December).

Durante meses y en algunos casos años, mucha gente y organizaciones involucradas en ciberdefensa y seguridad han reclamado una doctrina de ciberguerra que defina claramente las reglas de compromiso (ROE) necesarias para tratar esta amenaza. Mucho de ello está sin respuesta. Las reglas de ciberguerra, ciberespionaje, ciberterrorismo y otros actos de ciberagresión parecen estar hechos sobre la marcha. Una estrategia revelada en una reciente conferencia ilustra un punto de vista muy preocupante. Quizá dos de las áreas menos claras del escenario de las ciberamenazas son 1) qué constituye un acto de ciberguerra y 2) atribución de la responsabilidad. Esto conduce a la pregunta: ¿qué organización debería tomar la iniciativa cuando ocurren cibereventos y no está claro quién está detrás de ellos? Delincuentes, hackers, terroristas o estados paria – realmente no se sabe cuándo se producen estos eventos, por ello no puede determinarse si se trata de una cuestión de seguridad nacional o un tema militar.

Los ciberatacantes usan una topología de ataque multi-segmento. Hasta que se establezca la cooperación internacional en ciberinvestigación, la capacidad de atribuir un ataque a una entidad concreta será difícil. Mientras que la ciberinteligencia acompañada por la recopilación de la inteligencia tradicional proporcionará la procedencia y el mecanismo, la evidencia necesaria en un tribunal exigirá mucho más. Por ejemplo, aproximadamente un 32% de los ataques de denegación de servicio distribuido (DDoS) contra Estonia en 2007, así como un 35% del tráfico contra Georgia, se originó desde ordenadores comprometidos dentro de EEUU. Recientemente, el Centro de Seguridad de Tecnologías de la Información de Georgia estimó que un 15% de los ordenadores conectados mundialmente han estado comprometidos y han sido parte de botnets. Esto arrojaría un número de bots de aproximadamente 300 millones con lo cual se ilustra el problema de la atribución del ataque.

Respecto a las cibercapacidades, múltiples artículos aparecidos plantean la posibilidad de una carrera ciberarmamentística. Hay poca duda de que esta carrera ya ha comenzado. De hecho, este análisis sugiere que la carrera ciber comenzó en 2004. Además las características únicas de las ciberarmas las hacen amorfas, básicamente eliminan el uso de enfoques tradicionales para el control de armas y reduce enormemente o torna inútil muchas de las capacidades de recopilación de inteligencia tecnológicamente sofisticada que normalmente se usa para estimar y verificar las capacidades militares de los enemigos.

El desarrollo, adquisición y uso de las capacidades de ciberataques exigen que los gobiernos, militares y el sector tecnológico tomen acciones

decisivas para mitigar los riesgos. Un número significativo de naciones están incorporando la ciberguerra como una nueva parte de su doctrina militar. Actualmente, aproximadamente 160 países en el mundo están examinando de forma activa y concienzuda las capacidades de ciberguerra. EEUU, Rusia y China lideran esta carrera seguidos por India, Irán, Corea del Norte, Japón e Israel. Esta clasificación puede cambiar rápidamente debido al mercado negro en Internet de las modernas cibercapacidades.

Como conclusión, un cierto número de informes no clasificados han encontrado que al menos EEUU está en riesgo de ser incapaz de repeler un ciberataque a menos que refuerce su ciberseguridad. Tratar la amenaza de un ciberataque será mucho más difícil que controlar el desarrollo y propagación de las armas nucleares. La capacitación, equipo y materiales que se necesitan para crear ciberarmas son minúsculos en comparación con lo exigido para producir un dispositivo nuclear. Las propiedades novedosas de las ciberguerras están revolucionando la manera de hacer la guerra y de ejecutar las operaciones de espionaje. Dados los esfuerzos actuales y futuros de los delincuentes, extremistas, terroristas, naciones parias y militares de todo el mundo, un ordenador, sistema o red desprotegido es un ciberarma esperando a ser cargada y utilizada, y hasta que aceptemos esta premisa, estamos todos bajo riesgo.

El tema de la ciberseguridad y el nivel de amenaza actual que suponen los ciberataques no son exagerados. Si la complejidad del entorno de los ciberconflictos no fuera suficientemente alto, hay que añadir los temas de las relaciones externas creadas durante las investigaciones de los ciberataques, las complejidades de las leyes internacionales y la dificultad de atribuir un ciberataque y sumar además, todo el tema político que rodea a un ciberconflicto, estableciendo una política internacional, que cubra la doctrina militar y las leyes gubernamentales. Todo esto retrasará que se ultime una respuesta apropiada a los actos de ciberagresión.

Las características únicas de la ciberamenaza, su evolución continuada y las implicaciones potenciales de un ataque, hacen que lo que lleva años ahora se deba hacer en meses, lo que lleva meses se deba hacer en días, lo que lleva días deba hacerse en horas y lo que lleva horas deba hacerse en minutos. Las medidas de seguridad actuales se han mostrado inadecuadas contra las avanzadas ciberarmas que han evolucionado en pocos años. Los esfuerzos de investigación adicionales deben centrarse en eliminar los errores de código que crean vulnerabilidades durante el desarrollo del código, así como centrarse en el área de

las pruebas de vulnerabilidades de seguridad y en el área de garantía del código y los sistemas completos.

Se han observado dos posturas nacionales diferentes respecto al riesgo en el ciberespacio. Por un lado, el temor a las catastróficas consecuencias de un hipotético «ciber-Katrina» o a un «ciber-11S» ha provocado que países como EEUU, Francia, Reino Unido, Israel y Corea del Sur, así como la ONU y la OTAN entre otras organizaciones, hayan tomado conciencia de la importancia y necesidad de un ciberespacio seguro y, por ello, han desarrollado marcos normativos, planes y estrategias específicos para la defensa del ciberespacio (51). Por otro lado, China, Irán, Corea del Norte, Rusia y Pakistán han reconocido su interés estratégico en el ciberespacio como vehículo para alcanzar posiciones de liderazgo económico y político en sus áreas geográficas de influencia, y lo están concretando en la definición de políticas y en la ejecución de grandes inversiones económicas destinadas a recursos TIC y la formación de recursos humanos, con el objetivo de establecer «una defensa beligerante» de su ciberespacio. Estos países, o al menos sus territorios, han sido identificados como el origen de la mayoría de las acciones agresivas acontecidas en el ciberespacio durante los últimos años.

CONCLUSIONES

La ciberseguridad afecta al bienestar digital de la sociedad, de las organizaciones y de los países. Dentro de la sociedad afecta a distintas dimensiones: dimensión política, social, económica, legal, justicia y policial, técnica y de gestión. Los desafíos son complejos y satisfacerlos requiere de la voluntad política para diseñar e implementar una estrategia global para el desarrollo de infraestructuras de información que incluyan una estrategia de ciberseguridad coherente y efectiva. Una respuesta firme a las dimensiones humana, legal, económica y tecnológica de las necesidades de seguridad de infraestructuras de información puede construir confianza y genera un crecimiento del bienestar económico que beneficie a toda la sociedad.

Parece ya claro por lo expuesto anteriormente que la seguridad del ciberespacio es un objetivo estratégico de la seguridad nacional. El impacto de una amenaza sobre el ciberespacio tiene implicaciones sociales y económicas en el país. La próxima Estrategia Española de Seguridad deberá contemplar la seguridad en el ciberespacio (como ya se han plan-

(51) Fojón Enrique y Sanz Ángel, opus citatum.

teado algunos países de nuestro entorno (52)) y constituir el punto de partida de una Estrategia Nacional de Ciberseguridad, marco normativo a su vez, regulatorio de la seguridad en el ciberespacio. Posteriormente, debería centralizarse la gestión de la ciberseguridad con la creación de un organismo responsable de coordinar a todas las entidades públicas y privadas implicadas en España (53). Todo ello sin olvidar la cooperación internacional en esta materia y fomentar una cultura de ciberdefensa y una promoción de la I+d+i en el sector de la ciberseguridad. Los viejos problemas siguen estando presentes en esta sociedad de la información y las tecnologías y debemos servirnos de las nuevas tecnologías para buscar soluciones a los mismos.

BIBLIOGRAFÍA

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una Agenda Digital para Europa.

Estrategia Europea de Seguridad (EES) de 2003.

Estrategia de Seguridad Interior de la UE de 2010

Estrategia de Tecnología e Innovación para la Defensa, ETID-2010. Ministerio de Defensa. Dirección General de Armamento y Material. Subdirección General de Tecnología y Centros.

European Commission. Glossary and Acronyms (Archived). In Information Society Thematic Portal.

Fojón Enrique y Sanz Ángel. «*Ciberseguridad en España: una propuesta para su gestión*», Análisis del Real Instituto Elcano, ARI Nº 101/2010

Geers, Kenneth, «*The Cyber Threat to National Critical Infrastructures: Beyond theory*«. Information Security Journal: A global perspective, 18:1-7, 2009.

Gibson, William. «*El Neuromante*». (1984).

Guía de seguridad de la STIC (CCN-STIC-401), Glosario y abreviaturas, 1 de febrero de 2010.

(52) El gobierno británico ha publicado la Estrategia de Seguridad Nacional, en cuyas prioridades destaca la lucha contra el terrorismo y la ciberseguridad, entre otras. A Strong Britain in an Age of Uncertainty: The National Security Strategy. HM Government. TSO (The Stationery Office). www.tsoshop.co.uk. Fecha consulta 20.10.2010.

(53) Fojón Enrique y Sanz Ángel, opus citatum.

Informe de Amenazas CCN-CERT IA-03/10. Ciberamenazas 2009 y tendencias 2010.

Joint Publication 1-02. Department of Defense Dictionary of Military and Associated terms. (2009) [on line], http://www.dtic.mil. Fecha consulta 3.11.2009.

Joyanes, Luis. «*Cibersociedad. Los retos sociales ante un nuevo mundo digital*». Ed. McGraw-Hill. 1997.

Kevil Coleman, «*The weaponry and strategies of digital conflict*». Security and Intelligence Center at the Technolytics Institute, USA, 2010.

Lewis, J. A., «*Assessing the risks of cyber terrorism, cyber war and other cyber threats*», Center for Strategic and International Studies. (2002 December).

Marios Panagiotis, «*Challenging NATO's Security Operations in Electronic Warfare: The policy of Cyber-Defence*». 2009.

Masana, Sebastián. «*El ciberterrorismo: ¿una amenaza real para la paz mundial?»,* Tutor: Carlos Escudé. Facultad Latinoamericana de Ciencias Sociales, 2002.

Moore, D. and Paxson, V. and Savage, «*Inside the Slammer Worm*». IEEE Security and Privacy. 2003.

Ottis, Rain and Lorents, Peeter. «*Cyberspace: definition and implications*». Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2010.

Ottis, Rain, «*Proactive Defense Tactics against on-line cyber militia*». CCD-CoE. Tallinn, Estonia. 2010.

Rain, Ottis and Lorents Peeter. «*Cyberspace: Definitions and Implications*», Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. 2010.

Sánchez Medero, Gema. «*Ciberguerra y ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica*». Amérigo Cuervo-Arango, Fernando; Peñaranda Algar, Julio. «*Dos décadas de Posguerra Fría»*. Instituto Universitario General Gutiérrez Mellado, 2009. Tomo I, p. 215-241.

The Comprehensive National Cybersecurity Initiative. 2009.

Umphress, David A. «*El Ciberespacio. ¿Un aire y un espacio nuevo?», Air & Space Power Journa*l. Tercer Trimestre 2007.