INTRODUCCIÓN.
ESTADO DEL ARTE DE LA CIBERSEGURIDAD

INTRODUCCIÓN. ESTADO DEL ARTE DE LA CIBERSEGURIDAD

LUIS JOYANES AGUILAR

RESUMEN

En esta introducción se analiza el estado del arte de la Ciberseguridad así como el concepto de ciberguerra dentro del ciberespacio como quinto dominio de la guerra junto a la tierra, mar, aire y espacio. Se describe el nuevo modelo de computación en nube piedra angular de las nuevas infraestructuras tecnológicas de esta década así como las tecnologías más disruptivas de la actualidad de impacto en las ciberamenazas y en consecuencia en las ciberdefensas (realidad aumentada, geolocalización, Web en tiempo real, Internet de las cosas,…). La ICANN organismo internacional regulador de los sistemas de nombre de dominio (DNS) ha aprobado recientemente el protocolo de seguridad DNSSEC para asegurar una protección más completo de dichos sistemas ante los posibles agujeros en su seguridad. Se describe el estado actual de la ciberseguridad desde la perspectiva de organizaciones y empresas junto con una descripción de los organismos españoles con competencias en ciberseguridad.

En la parte II se describen los objetivos de la obra y una síntesis de los contenidos realizados por los respectivos autores de sus diferentes capítulos así como los retos, amenazas y oportunidades que plantea la ciberseguridad.

Palabras clave: Ciberespacio, Ciberguerra, Ciberamenazas, Ciberataques, Ciberseguridad, Cibercrimen-Ciberdelito, Ciberespionaje, Computación en Nube, ICANN, DNS, DNSSEC.

ABSTRACT

This overview examines the state of the art of cyber security and the concept of cyber war in cyberspace as the fifth domain of war with the land, sea, air and space. Describes the new model of cloud computing cornerstone of the new technological infrastructure of this decade and most disruptive technologies of today's cyber threats impact and consequently in cyber defense (augmented reality, geolocation, real-time Web, Internet of things The ICANN regulatory international organization of the domain name system (DNS) has recently approved the security protocol DNSSEC to ensure more complete protection complete of the above mentioned systems before the possible holes in his safety. Describes the current state of cyber security from the perspective of organizations and companies along with a description of the Spanish institutions with competence in cyber security.

Part II describes the objectives of the work and a summary of the contents made by the various authors of different chapters and the challenges, threats and opportunities posed by cyber-security.

Keywords: Cyberspace, Ciberwar-CyberWarfare, Cyber Threats, Cyber Attacks, Cyber Security, Cyber Crime, Cyber Espionage, Cloud Computing, ICANN, DNS, DNSSEC

I PARTE. La Ciberseguridad en la Defensa Nacional

INTRODUCIÓN A LA CIBERGUERRA (*Cyberwar – Cyberwarfare*)

«*Cyberwar. The thread from the Internet*», la portada y «*Cyberwar*» el título de la editorial del primer número del mes de julio de 2010 (1) de la prestigiosa revista británica ***The Economist*****,** esta revista de referencia mundial en economía y en los negocios quería destacar que era el momento de que los países comienzan a dialogar sobre el control de las armas cibernéticas en Internet.

El editorial (2) comienza analizando como a través de la historia las nuevas tecnologías han revolucionado la guerra, a veces abruptamen-

(1) *The Economist*. Volume 396 number 8689, July 3rd-9th 2010.

(2) La revista plantea el tema de la ciberguerra con un editorial (pp. 9-10) y un extenso *dossier* (*briefing cyberwar*) «Guerra en el quinto dominio» (*War in the fifth domain,* pp.

te, a veces sólo gradualmente; pensemos en el carro de combate, en la pólvora, el avión, el radar o la fusión nuclear. Igual que ha sucedido con las Tecnologías de la Información. Las computadoras e Internet han transformado la economía y han dado grandes ventajas a los ejércitos occidentales tales como la capacidad de enviar aviones controlados remotamente para capturar inteligencia o atacar a objetivos. Sin embargo, como reconoce *The Economist* la expansión de la tecnología digital tiene sus riesgos al exponer a los ejércitos y a la sociedad a los ciberataques (ataques digitales). La amenaza es compleja, en múltiples aspectos y potencialmente muy peligrosa. Al igual que ha sucedido con el control de las armas convencionales y nucleares, los países occidentales deben comenzar a pensar en el modo de reducir las amenazas de la ciberguerra con el objetivo de intentar evitar los ataques antes de que sea demasiado tarde o afrontarlas con éxito si se realizan.

LA CIBERGUERRA EN LOS MEDIOS DE COMUNICACIÓN

Las noticias de ciberataques a ciudadanos, organizaciones, empresas y, hasta, instalaciones críticas de países como plantas de energía química, centrales nucleares o fábricas de diferentes índoles se han vuelto habituales en los diferentes medios de comunicación no sólo escritos, sino radio, televisión y, naturalmente, los medios electrónicos de Internet. Hemos hecho una breve recopilación de noticias de actualidad relativas a la ciberguerra y seguridad recogidas en la prensa española e internacional de los últimos meses y que nos pueda servir de breve introducción a la actualidad del tema central de nuestra obra.

Noticias de actualidad

El Ejército de Brasil y la empresa española de seguridad Panda Security juntos contra la ciberguerra (3)

«Panda Security firmó un acuerdo a finales de octubre de 2010 con el Ejército de Brasil para apoyar a la institución en la profesionalización de sus capacidades operacionales en la lucha contra el ciberterrorismo,

---

22-24) donde analiza más detenidamente el ratón y el teclado de una computadora como las posibles «armas cibernéticas» del mundo en que vivimos, sus amenazas y los riesgos que conllevan.

(3) *El Mundo,* 4 de octubre de 2010, p. 36.

los crímenes virtuales y su preparación estratégica para potenciales intervenciones en caso de guerra cibernética» (*El Mundo 2010*). El acuerdo se ha realizado entre Panda Security y el Centro de Comunicaciones de Guerra Electrónica del Ejército de Brasil (CCOMGEX) y busca trabajar conjuntamente en la formación de primer nivel del personal del Ejército así como en la investigación científica y forense de los cibercrímenes tratando de dar respuesta en menos de 24 horas a todos aquellos códigos dañinos (maliciosos) que afecten fundamentalmente a Brasil.

Esta noticia saltó a los medios de comunicación españoles y brasileños pero cada día abundarán las colaboraciones entre empresas fabricantes y distribuidoras de soluciones de seguridad informática y ejércitos nacionales de diferentes países.

Irán sufre un ataque informático contra sus instalaciones nucleares (4)

Cymerman (2010) en La Vanguardia, informa que Irán sufrió el 27 de septiembre de 2010, de confirmarse, el ataque cibernético más grande de la historia. Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, se vieron afectados por un virus de una potencia sin precedentes, denominado Stuxnet. Los expertos consultados afirman que el 60% de los ordenadores iraníes se podrían haber visto afectados, igual que el 20% en Indonesia y el 8% en India. El virus Stuxnet se convierte en agente durmiente y se puede accionar a distancia en el momento que su creador lo desee sin que el usuario sea consciente. Dada su complejidad sin precedentes es imposible que haya sido creado por un hacker en solitario. Todo apunta a un equipo de profesionales que han dispuesto de medios y dinero suficiente y al menos seis meses de tiempo para prepararlo.

Los expertos consideran que el Stuxnet es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas como centrales eléctricas y nucleares, presas e industrias químicas. «La complejidad del programa es tal que los especialistas en seguridad informática que lo han examinado están convencidos de que

(4) Ángeles ESPINOSA, *El País,* 28 septiembre de 2010, p. 6. Además de El País, ese día prácticamente toda la prensa nacional e internacional recogían la noticia: *Financial Times*, «Online attack was aimed at nuclear work, says Teheran», p. 2; *La Vanguardia*, «Irán sufre un masivo ataque informático», pp. 8-9; *ABC, El Mundo*, etc. fueron otros periódicos españoles que recogieron la noticia.

no puede ser obra de un mero pirata informático. La mayoría opina que hay un Estado detrás y que es el primer ejemplo de guerra cibernética» (Espinosa 2010) (5).

Israel militariza la cibernética (6)

«En Israel se cree que el virus Stuxnet que ha atacado a las instalaciones nucleares iraníes fue introducido por un especialista extranjero que se limitó a usar una memoria tipo lápiz electrónico USB que estaba preparado para infectar la red iraní» (Cymerman 2010). Probablemente comenta Cymerman nunca se sabrá de forma oficial y confirmada quien ha lanzado el ataque cibernético –el mayor de la historia– contra las instalaciones atómicas iraníes, pero lo que está claro es que en muchas capitales occidentales se mira hacia la zona de Gelilot, al norte de Tel Aviv, donde está situada la gran unidad de inteligencia militar conocida por sus iniciales Aman y que formada por cientos de soldados especializados en la guerra cibernética y que en la jerga de Aman se conoce como «las guerras del siglo XXI». La Inteligencia israelí como ya están haciendo otras organizaciones internacionales comienza a reclutar a grandes expertos en informática.

Señala Cymerman que los especialistas en ciberseguridad informática se aglutinan en torno a los sistemas estratégicos de Israel: el Ministerio de Defensa, las centrales nucleares de Dimona y Sorek, el Instituto Biológico de Nes Tsiona, las compañías de electricidad y de agua, los aeropuertos de Ben Gurion, de Sde Dov y de Eilat, y cientos de bases militares del país, por ejemplos, todas aquellas en las que están almacenados misiles.

Ataques a las páginas Web de la SGAE y Cultura

A mediados de octubre de 2010, miles de internautas lanzaron desde sus PC millones de ataques contra las webs de la Sociedad General de Autores y Editores (SGAE), el Ministerio de Cultura y la patronal discográfica Promusicae. Los convocantes, que protestaban contra el canon digital

(5) Ángeles ESPINOSA, «Irán sufre un ataque informático contra sus instalaciones nucleares» en *El País,* 28 de septiembre de 2010, p. 6.

(6) Henrique CYMERMAN. «Israel militariza la cibernética» en *La Vanguardia,* 12 de octubre de 2010, p. 4. Cymerman es un destacado periodista y analista de temas de Oriente Medio en medios de comunicación españoles y extranjeros, tanto escritos como de televisión y radio.

y la ley que perseguirá a las páginas de descargas no autorizadas, consiguieron su objetivo de tirar abajo durante horas las webs atacadas y una repercusión mediática que pocas manifestaciones callejeras consiguen.

Los organizadores, el grupo de ciberactivistas Anonymous, que actúan en su mayor parte desde Estados Unidos, plantearon el ataque a través de foros como 4chan y redes sociales, dentro de una campaña internacional contra las corporaciones que «coartan la creatividad» y la política de los «lobbies» de los derechos de autor y que le han llevado a tumbar anteriormente las webs de asociaciones estadounidenses como la cinematográfica MPAA y la discográfica RIA (Muñoz 2010) (7).

Anonymous es un grupo que ha protagonizado ataques cibernéticos muy famosos. No tiene ningún líder, se organizan y deciden sus acciones en foros como 4chan, y aunque se nutren de jóvenes y adolescentes, mayoritariamente en Estados Unidos, sus campañas son respaldadas por internautas de todas las edades y de muchos países. Saltaron a la fama con el asalto a la Iglesia de Cienciología, pero han protagonizado otras sonadas campañas contra el Gobierno australiano, contra sociedades de gestión de derechos, discográficas y estudios.

Con independencia de considerar la figura de los autores como ciberactivistas o como ciberdelincuentes, la consideración más importante en nuestro caso es que organizaciones o asociaciones como Anonymous, que en este caso estaba claro la intención de su protesta, podrían evidentemente cometer delitos cibernéticos que podrían afectar al funcionamiento de sitios web comerciales o de organizaciones públicas o privadas.

Existe gran dificultad de oponerse a estos ataques, ya que pocos servidores son capaces de aguantar simultáneamente un número masivo de peticiones como los 300 millones que recibió la Web de la SGAE en los tres días que duró «el ataque».

La Unión Europea prueba sus defensas en un simulacro de «ciberataque»

El 4 de noviembre de 2010, se realizó el primer ejercicio de simulación de un ciberataque llevado a cabo a nivel paneuropeo con el objetivo de mejorar la seguridad comunitaria frente a los ataques a las redes electró-

(7) Ramón MUÑOZ, ¿Ciberactivistas o ciberdelincuentes? En El País, 20 de octubre de 2010, pp. 30-31.

nicas. El ejercicio llamado «Cyber Europe 2010» ha sido impulsado por la Comisión Europea (CE) y pretendía hacer frente a piratas informáticos en un intento simulado de paralizar en varios estados miembros de la UE servicios en línea de importancia crítica.

El ejercicio fue organizado por los países de la Unión Europea con el apoyo de ENISA (8) (Agencia Europea de Seguridad de las Redes y de la Información) y del Centro Común de la Investigación (JCR) de la CE. Neely Kroes, vicepresidenta de la Comisión y responsable de la Agenda Digital Europea, visitó el centro de ataques del Reino Unido como acto preparatorio del ejercicio. A esta visita asistieron también representantes de información de los ministerios de comunicaciones, responsables de la protección de infraestructuras de información esenciales, organismos de gestión de crisis, equipos de respuesta a incidentes de seguridad informática, responsables de seguridad de la información y servicios de inteligencia en el campo de la seguridad.

El Centro de Control del Ejercicio se estableció en Atenas y asistieron 50 personas como participantes activos, como observadores o como directores del ejercicio. Adicionalmente intervinieron 80 personas desplegadas por toda Europa que actuaban bajo las instrucciones de los moderadores de Atenas y que a su vez podían contactar con otras personas de los estados miembros de la UE. Estuvieron implicadas más de 70 organizaciones europeas en el desarrollo del ejercicio.

El ejercicio ha nacido con la idea de continuidad en el tiempo; de hecho y de modo anecdótico parece que el logo diseñado por ENISA para el ejercicio será la imagen de Cyber Europe y solo habrá que cambiar en cada ocasión que se realice el año correspondiente.

¿Cuáles fueron los resultados de las pruebas? Las notas de prensa publicadas por ENISA el día 5 de noviembre hablan de que el ejercicio concluyó con «éxito». El ejercicio consistió en exponerse a más de 320 «incidentes» y tenía como objetivo fortalecer la ciberdefensa en Europa. El director ejecutivo de ENISA, Udo Helmbrecht, aseguró que es el primer paso para fortalecer la ciberprotección europea. Se trataba de analizar la respuesta a los incidentes y aprender de los errores como «lecciones aprendidas» de modo que los Estados miembros analicen e implementen adecuadamente los resultados y mejoren los canales y procedimientos de comunicación.

(8) www.enisa.europa.eu/publications/eqr

En el análisis de los datos, se informó que participaron más de 150 expertos de 70 organismos públicos de la UE pertenecientes a 22 Estados miembros y ocho países como observadores. En el experimento estuvieron implicados equipos de respuesta rápida informática, ministerios, autoridades reguladoras, etc. El miércoles 10 de noviembre se ha hecho público el informe final y un balance oficial.

En «el aire» del ejercicio subyacía la reciente aparición del gusano Stuxnet que se dirige a instalaciones industriales críticas y que a finales de septiembre se detectó en varios países, de modo especial en Irán. Estos incidentes han aumentado los temores de una ciberguerra en la que las bombas lógicas serán programas dañinos (maliciosos) que buscarán paralizar o destruir las conexiones y las infraestructuras críticas de un país anulando sus sistemas informáticos.

Piratean la página Web de la Marina Británica

El Mundo (9) que a su vez cita fuentes de la *BBC* (10) británica publicaba, en su número de 8 de noviembre de 2010, la suspensión temporal de la página de Internet de la Marina Británica, después de que fuera objeto de un ataque de piratas informáticos, según el Ministerio de Defensa británico. Un mensaje publicado en la página de Internet informaba de una situación anormal (11).

Según informó la BBC el ataque fue realizado por un *´hacker´* conocido como TinKode mediante el método Inyección SQL(12), un tipo de ataque que introduce código SQL (13) dentro de otro código SQL para alte-

(9) [en línea] www.elmundo.es/elmundo/2010/11/08/navegante/1289231632.htm. El titular del periódico *El Mundo* era: «´Piratean´ la página Web de la Marina Británica».

(10) [en línea] www.bbc.co.uk/news/technology-11711478. El titular de la BBC publicado el 8 de noviembre de 2010 en su edición electrónica era: «The Royal Navy's website has been hacked by a suspected Romanian hacker known as TinKode». Tanto *El Mundo* como la *BBC* informaron que el ataque realizado a la página Web de la Royal Navy se produjo el 5 de noviembre de 2010 y el citado *hacker* utilizó un método de ataque conocido como «SQL injection». El hecho fue confirmado por una portavoz de la Marina Británica.

(11) «El mensaje original era:»*Unfortunately the Royal Navy website is currently undergoing essential maintenance. Please visit again soon!*».

(12) Inyección SQL es un agujero de *vulnerabilidad informática* de programas escritos en el lenguaje de programación SQL y que se produce durante la validación de las entradas a la base de datos de una aplicación.

(13) SQL, lenguaje estándar de desarrollo de software para bases de datos.

rar su funcionamiento. El acceso a la Web se produjo el 5 de noviembre y aunque la web no se vio comprometida, como medida de precaución se suspendió temporalmente la página web de la Marina Real, entre otros motivos porque el hacker capturó información que había conseguido.

LA CIBERGUERRA EN EL SIGLO XX Y LA ACTUAL Y FUTURA EN EL ACTUAL SIGLO XXI

A lo largo del libro en varios lugares y en especial en el Capítulo 4 donde se trata la situación de la ciberseguridad en el ámbito internacional y en la OTAN se recogen situaciones que algunos especialistas como Jeffrey Carr (2010) y Richard Clarke (2010) junto al ya citado informe de *The Economist* recogen como actos de ciberguerra (cyber warfare).

Carr analiza y a lo largo de su obra detalla en profundidad los casos de ciberguerra de los siglos XX y XXI, destacando los siguientes: China, Israel, Rusia (engloba en este apartado los casos de la Segunda Guerra Rusia-Chechenia del periodo 1997-2001; la ciberguerra de Estonia (2007) y la Guerra Rusia-Georgia (2008)), Irán y Corea del Norte.

Economist refleja como Estados Unidos está preparándose para la Ciberguerra y como el Presidente Obama ha declarado la infraestructura digital de América sea «un activo estratégico nacional» y nombró a Howard Schmidt, antiguo jefe de seguridad de Microsoft, como su zar de ciberseguridad y posteriormente creó el Cyber Command (Cybercom) y nombró director al General Keith Alexander, director de la Agencia Nacional de Seguridad (NSA) con un mandato claro «conducir las operaciones de amplio espectro para defender las redes militares de Estados Unidos y los ataques si fuera necesario a los sistemas de otros países».

Richard Clarke, antiguo ejecutivo de contraterrorismo y ciberseguridad en Estados Unidos, ha publicado este año un libro de gran impacto mediático sobre la ciberguerra en el que prevé o se imagina un fallo catastrófico (breakdown) «en cuestión» de quince minutos. Se imagina que los errores de los ordenadores llevarán a la caída de los sistemas de correo electrónico militar; las refinerías y los oleoductos explotarán, los sistemas de control de tráfico aéreo se colapsarán; los trenes de pasajeros y de carga y los metros descarrilarán; las redes eléctricas de los Estados Unidos se caerán; las órbitas de los satélites quedarán fuera de control. Y lo que es peor de todo, la identidad del atacante puede ser un misterio.

Economist anticipa otro posible gran problema que se puede producir por la rotura de comunicaciones a nivel mundial. Aunque considera que dicha rotura es muy difícil ocurra dado que los datos se envían en Internet por múltiples caminos y numerosas alternativas, si constata que en algunos puntos la infraestructura digital global es frágil. Más de las nueve décimas partes del tráfico de Internet son submarinas, viajan bajo la superficie del mar a través de cables de fibra óptica y éstos son críticos en algunos lugares físicos, por ejemplo alrededor de Nueva York, el Mar Rojo o el estrecho de Luzón en Filipinas. Otros peligros que detecta The Economist son la fragilidad de algunos gobiernos en algunas partes de África que pueden crear refugios para los cibercriminales.

Otro tema de gran impacto es la expansión y penetración de la telefonía móvil que traerá nuevos medios de ataques cibernéticos. De igual modo el informe también analiza el problema de las posibles vulnerabilidades de los servidores de nombres de dominio que comentaremos con más detalle en el siguiente apartado. La razón de su importancia reside en que el tráfico de Internet está dirigido por 13 clusters (servidores raíz) potencialmente vulnerables y que de hecho han recibido amenazas serias, aunque por suerte ICANN el organismo internacional regulador de los sistemas de nombres de dominio (DNS) ha resuelto prácticamente el problema con la implantación de un nuevo estándar.

Por último solo mencionar y resumir, dado que se estudiarán en profundidad en los siguientes capítulos, los componentes fundamentales que son fundamentales para la evaluación del complejo dominio del ciberespacio: la ciberguerra, los ciberdelitos, las ciberamenazas, el cibercrimen y el ciberespionaje. Será necesario definir las ciberamenazas que ayuden en la elaboración de planes estratégicos de ciberseguridad teniendo presente todos los términos anteriores.

CLOUD COMPUTING (LA COMPUTACIÓN EN NUBE) Y LAS INNOVACIONES DISRUPTIVAS: EL IMPACTO EN LA CIBERSEGURIDAD

La Computación en la Nube o Informática en la Nube (*Cloud Computing*) se ha convertido en un nuevo paradigma tecnológico de gran impacto social. La Nube (*The Cloud*) es el conjunto «infinito» de servidores de información (computadores) desplegados en centros de datos, a lo largo de todo el mundo donde se almacenan millones de aplicaciones

Web y enormes cantidades de datos (*big data*), a disposición de miles de organizaciones y empresas, y cientos de miles de usuarios que se descargan y ejecutan directamente los programas y aplicaciones de software almacenados en dichos servidores tales como Google Maps, Gmail, Facebook, Tuenti o Flickr. La Nube está propiciando una nueva revolución industrial soportada en las nuevas fábricas de «datos» (Centros de Datos, *Data Centers*) y de «aplicaciones Web (*Web Apps*). Esta nueva revolución producirá un gran cambio social, tecnológico y económico, pero al contrario que otras revoluciones será «silenciosa» al igual que lo ha sido la implantación de Internet y la Web en la Sociedad.

Esta nueva arquitectura se denomina «*informática en la nube o en nube*» o «*computación en la nube o en nube*» (*cloud computing*). Los datos y las aplicaciones se reparten en nubes de máquinas, cientos de miles de servidores de ordenadores pertenecientes a los gigantes de Internet, Google, Microsoft, IBM, Dell, Oracle, Amazon,…, y poco a poco a cientos de grandes empresas, universidades, administraciones, que desean tener sus propios centros de datos a disposición de sus empleados, investigadores, doctorandos, etc. (14).

No existe una definición estándar aceptada universalmente; sin embargo, existen organismos internacionales cuyos objetivos son la estandarización de Tecnologías de la Información y, en particular, de *Cloud Computing.* Uno de estos organismos más reconocido es el National Institute of Standards and Technology (**NIST**) (15) y su Information Technology Laboratory, que define la computación en nube (*cloud computing*) (16) como:

El modelo de la nube, según NIST, se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue. La nube en sí misma, es un conjunto de *hardware* y *software*, almacenamiento, servicios e interfaces que facilitan la entrada de la información como un servicio. Los servicios de la nube incluyen el soft-

(14) Luis JOYANES. *Icade,* nº 76, enero-abril, 2009, pp. 95-111.

(15) El NIST es una Agencia del Departamento de Comercio de los Estados Unidos. Dentro del NIST, el Computer Security Resource Center (CSRC) se encarga de los estándares de las Tecnologías de la Información y, en concreto, de Cloud Computing.

(16) En octubre de 2009, Peter Mell y Tim Grance, investigadores del NIST publicaron la norma (*draft*) de la definición de *cloud computing* y una guía del mismo, realizada en colaboración con la industria y el gobierno y titulada: «Effectively and Securely Using the Cloud Computing Paradigm» y que puede ser descargada en el sitio oficial del NIST: http://crsc.nist.gov/groups/SN/cloud-computing/cloud-computing-v25.ppt.

ware, infraestructura y almacenamiento en Internet, bien como componentes independientes o como una plataforma completa –basada en la demanda del usuario.

El NIST en el documento antes comentado además de dar la definición de la Nube, define los modelos de entrega y despliegue de servicios en la Nube más usuales que se ofrecen a los clientes y usuarios de la nube (organizaciones, empresas y usuarios) son: **PaaS** (Platform as a Service), plataforma como servicio, **IaaS** (Infrastructure as a Service), infraestructura como servicio y **SaaS** (Software as a Service), software como servicio. Por otra parte los modelos de despliegue que se pueden implementar en las organizaciones y empresas son: **nube privada, nube comunitaria, nube pública** y **nube híbrida**, aunque el modelo de *nube comunitaria* que propone el NIST no ha sido muy aceptado por la industria informática y los tres modelos más aceptados en la bibliografía técnica, proveedores, organizaciones y empresas son: *privada, pública* e *híbrida,* taxonomía que también nosotros proponemos.

Las tecnologías del futuro

La Nube ha sido posible gracias a tecnologías de *virtualización*, los modernos centros de datos con millares de servidores, las tecnologías de banda ancha y de gran velocidad de transferencia de datos para poder realizar las conexiones entre ordenadores a cifras nunca vistas, la proliferación de dispositivos de todo tipo con acceso a Internet, desde PCs de escritorio hasta *netbooks,* teléfonos inteligentes, tabletas electrónicas como *iPad* o libros electrónicos como los lectores de libros electrónicos (*ebook), etc.* y, naturalmente, todas las tecnologías de la Web 2.0 y la Web Semántica que han traído la proliferación y asentamiento de los *Social Media* (Medios Sociales) en forma de *blogs, wikis,* redes sociales, *podcast, mashups*, etc. que han facilitado la colaboración, participación e interacción de los usuarios individuales y de las organizaciones y empresas, en un ejercicio universal de la **Inteligencia Colectiva** de los cientos de millones que hoy día se conectan a diario a la Web.

A todas estas tecnologías hay que añadir las *disruptivas* que han ido naciendo con la década y hoy día ya ofrecen numerosas aplicaciones innovadoras y que se irán extendiendo por la sociedad y que como hemos comentado ya traerán infinidad de ventajas a todo tipo a organizaciones y empresas, pero será necesario un estudio tranquilo y profundo de *las amenazas que traerán consigo también a la ciberseguridad y en particular*

a la protección de datos y privacidad de las personas, organizaciones y empresas. Queda fuera de los objetivos de esta obra el análisis en profundidad de estas tecnologías pero si queremos dejar constancia de ellas con vistas a un análisis posterior y que deberán, sin lugar a dudas, ser tenidas en cuenta en futuras estrategias de ciberseguridad por las posibles amenazas que conllevarán ya que como innovaciones tecnológicas y muy avanzadas que son atraerán a los cibercriminales y terroristas, en su caso, para aprovechar en su beneficio estas grandes aportaciones tecnológicas. Las tecnologías de mayor impacto son:

- **La Web en tiempo real** (búsqueda de información en redes sociales y *microblogs* como Facebook o Twitter que proporcionan datos de acontecimientos de todo tipo que se están produciendo en cualquier parte del mundo y en el momento que realizamos la búsqueda).
- **Geolocalización.** Gracias a los sistemas GPS instalados en los teléfonos inteligentes y a la conexión a redes inalámbricas o móviles 3G y las futuras 4G, se pueden asociar las coordenadas geográficas del lugar donde se encuentra el usuario de un teléfono para mostrar en la pantalla del dispositivo todo tipo de información sobre restaurantes, hoteles, espectáculos, etc., de lugares próximos a la posición geográfica incluso señalando distancias kilométricas a esos lugares (Ver sitios Web como Foursquare. Gowella,..).
- **Realidad Aumentada.** Mezclar la realidad con la virtualidad de modo que el usuario pueda, p.e., asociar la fotografía de un monumento a su historia, sus datos turísticos o económicos de modo que pueda servir para tomar decisiones tanto de ocio como para negocios, gestión del conocimiento de las organizaciones, etc. (*Googles* de Google, *Layar, Places* de Facebook, *Lugares* de Android, etc.).
- **Internet de las cosas.** Cada día aumenta el número de dispositivos de todo tipo que proporcionan acceso a Internet. Las «cosas» que permiten y van a permitir estos accesos irá aumentando con el tiempo. Ahora ya tenemos videoconsolas, automóviles, trenes, aviones, sensores, aparatos de televisión,… y pronto el acceso se realizará desde los electrodomésticos o desde «cosas» cada vez más diversas.

Las tecnologías anteriores serán posibles por nuevas tendencias relevantes que nos traerá el futuro cercano y que sintetizamos centrándonos en aquellas que más afectarán al nuevo cambio social que nos traerá

la nueva revolución industrial de los centros de datos (las fábricas de datos) y la computación en nube, y que resumiremos en las siguientes:

La difusión masiva que se está produciendo de la computación en nube unido a la creciente implantación de las tecnologías anteriormente citadas y otras muchas, están trayendo grandes beneficios a organizaciones y empresas de toda índole, pero a la vez están produciendo grandes problemas de seguridad y de protección de datos y privacidad que será preciso afrontar. Algunos informes rigurosos de empresas del sector de la seguridad informática consideran que a las grandes ventajas que traen consigo podrán traer grandes riesgos y amenazas contra la ciberseguridad, simplemente porque su facilidad de uso puede traer consigo la difusión de todo tipo de virus y amenazas de muy diversa índole.

Algunas amenazas (actuales y futuras)

La valoración de las amenazas actuales y futuras es una parte importante de la evaluación de las prioridades a tener en cuenta en las crecientes medidas de seguridad. Será preciso tener presente la prevención, detección, respuesta, mitigación y recuperación junto con la cooperación internacional en su caso. Describiremos brevemente algunas de las amenazas que se han hecho más «populares» en los últimos tiempos por las repercusiones e impacto que han tenido en aquellos lugares y equipos donde se han producido.

Stuxnet

Es un programa de software dañino (malicioso) del tipo *troyano* muy avanzado, que aprovecha la vulnerabilidad MS10-0466 de los sistemas operativos Windows CC, empleados en los sistemas SCADA (*Supervisory Control and Data Acquisition*) fabricados por Siemens y que se utiliza en infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos. Se piensa que una vez dentro de una planta podría reprogramar las centrifugadoras para hacerlas fallar sin que se detectara.

Stuxnet es un virus muy sofisticado que utiliza técnicas de *rootkit* para instalarse en el sistema operativo. El troyano queda camuflado y latente en el equipo infectado hasta que su autor decide activarlo.

Se detectó el mes de junio de 2010 por una compañía de seguridad informática de Bielorrusia, VirusBlokAda que lo descubrió en unos ordenadores pertenecientes a un cliente en Irán. Entonces se pensó que se trataba de un programa dañino diseñado para robar procesos de fabricación o bocetos de productos; sin embargo después del ataque de septiembre se piensa que ha sido creado para sabotajes de infraestructuras críticas de las naciones. Este tipo de troyanos no van destinados a la infección masiva de ordenadores domésticos sino que está pensado para atacar a infraestructuras críticas o incluso sabotajes industriales, donde puede aumentar o disminuir el caudal de un oleoducto o dañar a una central nuclear. Dado que va dirigido contra infraestructuras críticas que no utilizan Internet, se supone que el troyano se introdujo en los ordenadores a través de lápices de memoria tipo USB y luego se multiplica a sí mismo, pasando de un ordenador a otro, instala programas troyanos de espionaje para recoger información y puede dañar tanto sitios web como sistemas operativos.

Según Eugene Kaspersky (17), fundador de la compañía de seguridad informática que lleva su nombre y que fue la primera en detectar la amenaza, «durante décadas hemos visto ataques de cibervándalos y ciberdelincuentes; acabamos de entrar en la era del ciberterrorismo». Por su precisión, continua Kaspersky, «Stuxnet no puede haber sido creado por ningún grupo de hackers, solo algunos estados tienen recursos para montar una operación semejante».

DDoS

Los ataques DDoS (Distributed Denial of Service) son una forma relativamente sencilla y efectiva de hacer caer a una Web. Las acciones se pueden realizar de forma voluntaria siguiendo las instrucciones dadas para iniciar el ataque a una hora señalada en una convocatoria mediante foros en la Red o utilizando redes de ordenadores previamente infectados por virus (*botnet*) de forma que los usuarios ni siquiera son conscientes de que participan.

Los ataques DDoS no siempre tienen un trasunto ideológico. Cada vez más responden a puras extorsiones. Se están trasladando a Internet los mismos esquemas que empleaba la mafia en el mundo físico.

(17) Declaraciones en *La Vanguardia*, suplemento *Dinero*, sección de Tecnología, Norberto Gallego, p. 16, 10 de octubre de 2010.

Botnets

Los botnets (robots de la Red) son redes de ordenadores zombis. Las redes han aumentado de modo exponencial, según informes de la Fundación Shadowserver y se emplean para realizar ataques, envíos masivos de correo basura y espionaje contra empresas. Un botnet se crea infectando ordenadores sin que sus propietarios lo sepan. Cada máquina reclutada por el virus se pone en contacto sigilosamente con el cibercriminal a la espera de sus órdenes.

Los ciberdelincuentes bien, de modo aislado, o en una organización, construyen sus *botnets* y los venden o alquilan a empresas que desean mandar correo basura, bombardear o espiar a otras empresas, o robar datos bancarios. El virus puede enviarse por correo electrónico aunque lo habitual es ponerlo en páginas web, fundamentalmente que tengan muchas visitas. Una vez dentro del ordenador, el virus descargará un programa y lo instalará, es el *bot,* el lazo entre el ordenador infectado y la *net,* la red que permite su control remoto.

Los botnets se usan mayoritariamente para el envío masivo de correo basura y virus, el bombardeo contra empresas y el espionaje, sea de empresas o de la información bancaria de los dueños de los ordenadores infectados. Otro método empleado por los creadores de los *botnets,* es el caso del fraude publicitario. El fraude consiste en crear una página cualquiera, poner en ella algunos anuncios legales y hacer que todos los ordenadores de la botnet los visiten. A efectos prácticos en las estadísticas se verá que los clics provienen de cientos o miles de direcciones IP diferentes, repartidas por todo el mundo y por tanto parecerá que son usuarios legítimos y no una estafa, de esta forma el anunciante deberá pagar el porcentaje convenido.

Zeus

Zeus es un virus de tipo botnet (troyano) que se propaga por los navegadores, tanto Explorer como Firefox. El malware recopila información del usuario y contraseñas de internet y redes sociales, utilizándolas para suplantar la identidad y realizar robo de datos bancarios, datos de tarjetas de crédito o enviar spam. Miles de empresas de todo el mundo han caído en esta pandemia digital. Además a primeros de noviembre de 2010 se ha detectado que el virus Zeus ha afectado a dispositivos móviles.

Uno de los grandes peligros es que el ataque Zeus ha conseguido propagarse por las redes sociales hasta obtener 10 millones de dólares de un banco en sólo 24 horas introduciendo malware en el ordenador personal del tesorero a través de una web infantil a la que accedió su hijo, contó a *Cinco Días* (18), Pilar Santamaría, directora de Desarrollo de Negocio y Ciberseguridad para la región Mediterráneo de Cisco, el gigante estadounidense de las comunicaciones Cisco.

Amenazas futuras

De acuerdo a un informe reciente de Cisco que comentaremos posteriormente, destaquemos ahora que en opinión de esta multinacional de las comunicaciones el futuro de las amenazas se centran en dos grandes áreas: ingeniería social (manipulación de formularios, llamadas no solicitadas, mensajes,…) y ataques multivectoriales donde se combinan diferentes tipos de soporte (correo electrónico, mensajes en blogs, redes sociales, wikis,…., voz, vídeo, audio, etc.).

EL CIBERESPACIO, EL QUINTO DOMINIO DE LA GUERRA

El Diccionario de la Real Academia Española (DRAE) en su 22ª edición define Ciberespacio, única acepción, como el «Ámbito artificial creado por medios informáticos». En realidad, entendemos que la RAE se está refiriendo a un entorno no físico creado por un equipo informático con el objetivo de interoperar en una Red. El mayor ámbito del ciberespacio es Internet.

El término fue utilizado por primera vez en la obra Neuromante del escritor norteamericano William Gibson y publicada en el emblemático *1984* que presagia Orwell. También podríamos definir el ciberespacio desde su perspectiva original como un conjunto o realidad virtual donde se agrupan usuarios, páginas web, chat y demás servicios de Internet además de otras redes. Otro nombre influyente en la definición e historia posterior del ciberespacio es John Perry Barlow, autor del famoso Manifiesto «*La declaración del Ciberespacio*» que se convirtió desde su aparición en referencia obligada al tratar el término y su impacto social. Barlow, declaraba el ciberespacio entre diferentes acepciones: «Alucina-

(18) Declaraciones de Pilar Santamaría, Directora de Desarrollo de Negocio y Ciberseguridad de Cisco Mediterráneo, en un artículo de Manuel G. Pascual, en *Cinco Días*, 10 de noviembre de 2010, p.14.

ción sensual», «Espacio virtual de interacción» o «el nuevo hogar de la Mente». Sin embargo, la definición más sencilla y práctica dada en los nacimientos del concepto es «Un espacio virtual de interacción» o de un modo simple: «Aquel espacio donde sucede una conversación telefónica». Hoy podríamos extender esta definición a: «El espacio donde se navega por Internet, se realizan conversaciones por Skype o en las redes sociales, o estamos cuando consultamos el correo electrónico, chateamos o visitamos un periódico digital».

Existen numerosas definiciones de ciberespacio. Desde la más simple y ya vieja e histórica «es aquel espacio donde sucede una conversación telefónica», hasta una más práctica y actual «El espacio o realidad virtual donde se agrupan usuarios, páginas web, chat, redes sociales, blogs,… y demás servicios de la Web y de Internet». En cualquier caso y relativo al tema central de esta obra, «el ciberespacio es el nuevo campo donde pasamos gran parte de nuestras vidas los más de 1.000 millones de habitantes que hoy día tenemos acceso a Internet»; este campo, es un gran campo social donde disfrutar, trabajar, pensar, vivir,…, pero también es un *nuevo campo de batalla,* debido a los riesgos y amenazas que su uso masivo plantea.

El ciberespacio fue declarado por *The Economist* (19) como el quinto dominio después de la tierra, el mar, el aire y el espacio. El presidente de Estados Unidos, Barack Obama, ha declarado que la infraestructura digital de América debe ser declarada «un activo nacional estratégico» y para conseguir ese objetivo nombró a Howard Schmidt, antiguo director de seguridad de Microsoft, como su zar de la ciberseguridad. En mayo de 2010 el Pentágono estableció su nuevo Cyber Command (Cybercom) nombró director del mismo al general Keith Alexander, director de la National Security Agency (NSA), habiendo quedado activado Cybercom en el pasado mes de octubre. Su mandato le obliga a conducir las operaciones de un amplio espectro para defender las redes militares estadounidenses y dirigir y realizar los ataques que fueran necesarios contra otros países.

La defensa del nuevo dominio. La ciberestrategia del Pentágono

Apoyándose en las estrategias marcadas al principio del mandato del Presidente Obama entre el año 2009 y 2010, William J. Lynn III (20), U. S, Deputy Secretary of Defensa, ha publicado un artículo en la prestigiosa

(19) *The Economist*, op. Cit., p. 22.
(20) William J, Lyns. *Foreign Affairs*, vol. 89, nº 5, septiembre/octubre de 2010, pp. 97

revista *Foreign Affairs*, donde expone los cinco principios básicos de la estrategia de la guerra del futuro:

- El ciberespacio debe ser reconocido como un territorio de dominio igual que la tierra, mar y aire en lo relativo a la guerra.
- Cualquier posición defensiva debe ir «más allá» del mero mantenimiento del ciberespacio «limpio de enemigos» para incluir operaciones sofisticadas y precisas que permitan una reacción inmediata.
- La defensa del ciberespacio (ciberespacial) debe ir más allá del mundo de las redes militares –dominios.mil y.gov. del Departamento de Defensa, para llegar hasta las redes comerciales (dominios. com,.net,.info,.edu, etc.) y que deben estar subordinados al concepto de Seguridad Nacional.
- La estrategia de la Defensa Ciberespacial debe realizarse con los aliados internacionales para una política efectiva de «alerta compartida» ante las amenazas mediante establecimiento de ciberdefensas con países aliados.
- El Departamento de Defensa debe contribuir al mantener e incrementar el dominio tecnológico de Estados Unidos y mejorar el proceso de adquisiciones y mantenerse al día con la agilidad que evoluciona la industria de las Tecnologías de la Información.

Estrategias de la ciberguerra en otros países

Numerosos países están estableciendo políticas de ciberseguridad. Así Gran Bretaña ha creado el GCHQ, un centro de operaciones equivalente de la NSA (National Security Agency) estadounidense. Ian Lobban, director del GCQH en un discurso pronunciado el 26 de octubre de 2010 pronunció las siguientes palabras: «Los países ya están usando técnicas de guerra cibernética para atacarse entre sí y necesitan estar alerta en todo momento para proteger los sistemas informáticos. El ciberespacio se disputa cada día, cada hora, cada minuto, cada segundo. La expansión del ciberespionaje ha elevado el riesgo de interrupción de infraestructuras como estaciones eléctricas y servicios financieros. La amenaza es real y creíble». Lobban en este discurso planteaba la existencia real de peligros en el ciberespacio.

China piensa en las guerras de la segunda mitad del siglo XXI. Muchos otros países están organizándose para la ciberguerra; entre ellos, Rusia, Israel, Corea del Norte, etc. El ciberespacio, ciertamente, formará parte de cualquier guerra que se produzca en el futuro.

The Economist, plantea que los datos actuales se envían por numerosas rutas, pero la infraestructura digital global todavía es muy frágil. Más de las nueve décimas partes del tráfico de Internet viaja por cables de fibra óptica debajo del mar y éstos pueden ser saboteados alrededor de Nueva York, el Mar Rojo o el estrecho de Luzón en las islas Filipinas. El tráfico de Internet está dirigido por 13 *clusters* de servidores de nombres de dominio, potencialmente vulnerables. Otros peligros pueden darse en las conexiones de cables de fibra óptica a través de países de África o de Asia. La masiva penetración del internet móvil está creando nuevos medios de ataques.

Los bancos y grandes compañías no les gusta admitir cuántos datos pierden diariamente, pero es una realidad palpable. En 2008 según fuentes de Economist, sólo la operadora de teléfonos Verizon de EEUU reconocía la pérdida de 285 millones de registros de datos personales, incluyendo detalles de tarjetas de crédito y de cuentas bancarias. Cerca de las nueve décimas partes de los 140.000 millones de correos electrónicos que se envían a diario son spam; de estos el 16% contienen ataques de «phishing», fraudes bancarios, según la empresa de seguridad Symantec.

El *malware* es utilizado normalmente para robar contraseñas y otros datos, o abrir una puerta trasera «*back door*» a una computadora de modo que puedan ser tomados por otros externos. Tales máquinas «*zombie*» se pueden conectar a millares, sino millones de otros ordenadores alrededor del mundo para crear un «*botnet*». La estimación del número de ordenadores infectados puede superar los 100 millones (21). Los botnets se utilizan para enviar spam, difundir malware o lanzar ataques distribuidos de denegación de servicios (DDoS).

El ciberespionaje es el desastre más grande de la inteligencia desde la pérdida de los secretos nucleares a finales de la década de los 40, según comenta Jim Lewis del Centre for Strategic and International Studies, un *think-tank* con sede en Washington, DC, según cuenta *The Economist*. El siguiente paso tras penetrar en las redes para robar datos es *disrupt* o manipularlos. Si la información militar clave puede ser atacada, podrán ser inutilizados misiles balísticos. Los atacantes pueden preferir ir a por

(21) Consultar el mapa de direcciones IP infectadas en: team-cymru.org y telegeography.com. Según este mapa, en la fecha de 29 de junio de 2010, las regiones más infectadas serían el Este de Estados Unidos, Centroamérica y zona oriental de Brasil, Europa y Sudeste asiático junto con Japón y Corea.

información de logística militar no clasificada o incluso infraestructuras civiles. Una pérdida de confidencialidad en transferencia electrónica de datos financieros puede producir desastres económicos. Un desastre podría ser un ataque a las redes eléctricas. Sin electricidad y otros servicios críticos, los sistemas de comunicaciones, los cajeros automáticos dejarían de funcionar. Una pérdida de energía durante unos pocos días, puede producir daños económicos en cascada impredecibles.

Los expertos no se ponen de acuerdo sobre las vulnerabilidades de los sistemas que funcionan en las plantas industriales conocidos como *supervisory control and data acquisition* (SCADA). Cada vez más estas infraestructuras se están conectando a Internet elevando el riesgo de ataques remotos y los programas SCADA de las redes se vuelven más vulnerables a los ciberataques (22).

La OTAN ha sido consciente del riesgo de las ciberamenazas y creó un nuevo «concepto estratégico» que se adoptará a finales de este año (23). Para ello un panel de expertos liderado por Madeleine Albright, antigua Secretaria de Estado de Estados Unidos, realizó un informe en mayo de 2010 en el que consideraba que los ciberataques estaban entre las tres amenazas más probables a la Alianza. El siguiente ataque significativo bien puede ser la rotura de un cable de fibra óptica y puede ser lo bastante serio como para merecer una respuesta bajo las previsiones de defensa mutua contempladas en el artículo 5 (del Tratado de Washington).

El General Alexander planteó la posible necesidad de la militarización del ciberespacio para proteger el derecho a la privacidad de los americanos. El Cibercomando protege solo al dominio militar «.mil». El domino de gobierno «.gov» y el de infraestructuras corporativas como los «.com» son responsabilidad respectivamente del Departamento de Homeland Security y de las empresas privadas con apoyo de Cybercom. Las ciberarmas se pueden utilizar principalmente como adjuntas o complementarias de las armas convencionales en el teatro de operaciones. El ciberataque se puede utilizar como un arma militar pero normalmente estará limitada en tiempo y efecto aunque si se utilizan como armas de espionaje el tiempo no importa y los resultados pueden esperar.

---

(22) Sin duda el exhaustivo informe de The Economist era premonitorio y avisaba de los riesgos de los sistemas SCADA, como así fue en los ataques sufridos a finales de septiembre, por el virus Stuxnet, especialmente en Irán.

(23) La OTAN en la Cumbre de Lisboa celebrada el 20 de noviembre de 2010 aprobó la estrategia de ciberseguridad.

La disuasión en la ciberguerra es más incierta que en el caso de la estrategia nuclear, ya que en este tipo de guerra no hay destrucción mutua asegurada y la línea divisoria entre la delincuencia y la guerra es borrosa y por ende, la identificación de los computadores atacantes y lógicamente, mucho menos, las pulsaciones de los dedos en los teclados, como atribución del posible delito. *Economist* concluye que las ciberarmas pueden ser más efectivas en manos de los grandes estados aunque también pueden ser de gran utilidad para los terroristas.

LA ACTUAL SEGURIDAD EN INTERNET. DOMINIOS INFECTADOS Y EL NUEVO PROTOCOLO DE SEGURIDAD DNSSEC DE ICANN

La seguridad en Internet ha estado en un grave riesgo en los últimos años debido a los riesgos existentes en el sistema legal de registro de nombres de dominio, DNS que llegó a producir infecciones masivas de direcciones de sitios Web. El «agujero de seguridad» parece que se ha resuelto gracias a la investigación de ICANN, el organismo internacional regulador de los nombres de dominio, y el posterior diseño, construcción e implantación del protocolo de seguridad DNSSEC.

Dominios infectados (estadísticas)

La compañía de seguridad McAfee ha publicado a finales de octubre su último informe sobre los dominios más peligrosos de la Red. En este informe ha realizado un análisis exhaustivo de más de 27 millones de sitios Web comprobando si existían amenazas de tipo malware o spam, afiliaciones sospechosas o pop ups agresivos. McAfee ha utilizado la tecnología Trustedforce centrada en la protección de datos y que reúne más de 150 sensores localizados en 120 países. Como resultados más significativos del informe, destaca que la lista de los 5 dominios más peligrosos son:

1. .com (31,3%)
2. .info (30.7%)
3. .vn (Vietnam)
4. .cm (Camerún)
5. .am (Armenia)

Los resultados destacan que el dominio.com, el más utilizado en Internet es, a su vez, el dominio de mayor riesgo, lo que confirma la tendencia de los hackers de centrarse en los soportes y plataformas más

masivos. El informe también destaca que el riesgo en la Red ha aumentado desde el año pasado y los cibercriminales son más rápidos en atacar a sus víctimas y cambian de tácticas con gran frecuencia para no ser descubiertos.

El ICANN y el sistema de nombres de domino (DNS). El caso del envenenamiento masivo de direcciones

ICANN es una asociación sin ánimo de lucro fundada en 1998 cuyo objetivo es asegurar que Internet sea segura, estable e interoperativa. Esta asociación promueve la competencia y desarrolla políticas de identificadores únicos de Internet. ICANN no controla el contenido de Internet, no puede detener el correo basura y no gestiona los accesos a Internet pero gracias al sistema de nombres de dominio (DNS) Internet puede evolucionar y evoluciona a la velocidad que lo hace actualmente. El sistema de nombres de dominio asocia una dirección URL (nombre) con una dirección IP (una serie de números), es decir, un nombre o un número han de ser únicos. La dirección de Internet del sitio web de ICANN (www.icann.org) equivale a 192.0.34.163, o de otra forma las direcciones IP son las que utilizan los ordenadores, mientras los nombres de dominio son los que utilizan los usuarios. Eso significa que igual que no puede haber dos nombres de dominio iguales tampoco puede haber dos direcciones IP iguales. ICANN se encarga de la gestión de las direcciones IP evitando que se puedan producir repeticiones.

Surgieron problemas de envenenamiento masivo en el trafico de direcciones IP (24) que consistió en que los *hackers* o piratas informáticos «secuestraron» el Sistema de Nombres de Dominio DNS aprovechando un error en el sistema de asignación de direcciones de Internet y eso permitía redireccionar el tráfico de Internet a sitios falsos con lo que podían «robar» datos tales como números de cuentas bancarias, datos privados o contraseñas personales. Hace un tiempo se detectaron vulnerabilidades en el sistema DNS que permiten que un atacante fuerce el proceso de buscar una persona o buscar un sitio en Internet utilizando

(24) Dan Kaminsky es un informático estadounidense que descubrió por casualidad un error en el sistema de asignación de direcciones de Internet y que suponía un fallo en la Red. Este no era un fallo local sino que suponía un gran envenenamiento de la Red ya que apareció un agujero en la libreta de direcciones de Internet y por consiguiente se podía redireccionar el tráfico de Internet a sitios falsos.

su nombre. El objetivo del ataque es tomar el control de la sesión para, por ejemplo, enviar al usuario al propio sitio web fraudulento del atacante, con el fin de obtener los datos de la cuenta y la contraseña. Por esta razón y tras un periodo largo de investigación, ICANN ha implantado el protocolo de seguridad DNSSEC (25) (Extensión de seguridad del DNS) para resolver el problema que brinda la protección contra este tipo de ataques mediante la firma digital de los datos a fin asegurar que son válidos. A fin ales de julio de 2010, ICANN anunció que había implantado el protocolo de seguridad en los 13 servidores raíz (26) de modo que se puede comprobar que las direcciones visitadas son auténticas y no han sido alteradas gracias a la implantación del protocolo de seguridad DNSSEC en los servidores raíz.

ORGANISMOS E INSTITUCIONES ESPAÑOLAS CON COMPETENCIAS EN CIBERSEGURIDAD

La ciberseguridad en «España, a diferencia de otros países de nuestro entorno, no ha sido definida todavía en una legislación específica y completa en materia de ciberseguridad aunque si existe legislación distribuida en distintos ámbitos ministeriales pero no se desarrollado todavía una política común que refleje el ámbito nacional» y estratégico de la ciberseguridad» (27). El Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica fue regulado en el Real Decreto 2/2010, de 8 de enero, pero cubre únicamente las administraciones públicas. Existen otras leyes nacionales, europeas e internacionales que abordan la seguridad, tales como: Ley Orgánica de Protección de Datos (LOPD), la Ley General de las Telecomunicaciones (LOT) y la Ley de la Sociedad de la Información y Comercio Electrónico (LSI-CE).

---

(25) En www.icann.org/es/announcements/dnssec-qaa-09oct08-es.htm se puede consultar el documento '¿Qué es y por qué es tan importante'

(26) Los servidores raíz son entidades distintas, 13 servidores raíz o, más precisamente, 13 direcciones IP en Internet en las que pueden encontrarse a los servidores raíz (los servidores que tiene una de las 13 direcciones IP pueden encontrarse en docenas de comunicaciones físicas distintas). Las entidades encargadas de operar los servidores raíz son bastante autónomas, pero al mismo tiempo colaboraran entre sí y con ICANN para asegurar que el sistema permanece actualizado con los avances y cambios de Internet [definición de servidor raíz de ICANN] en www.icann.org/es/participate/what-icann-do-es.htm

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

Es necesaria la gestión de la ciberseguridad, además de en la administración pública, en otros sectores importantes de organizaciones, empresas, infraestructuras críticas y los ciudadanos. Los organismos e instituciones más sobresalientes tienen competencias en la gestión de la ciberseguridad son (Fojón, Sanz 2010).

- El Centro Criptológico Nacional (CCN) dependiente del Centro Nacional de Inteligencia (CNI) que tiene a su cargo la gestión de la seguridad del ciberespacio en las tres administraciones del Estado.
- El CCN-CERT es el Centro de alerta nacional que coopera con todas las administraciones públicas para responder a los incidentes de seguridad en el ciberespacio y vela también por la seguridad de la información nacional clasificada.
- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) que depende del Ministerio del Interior.
- El Instituto Nacional de Tecnologías de la Comunicación (INTECO) dependiente del Ministerio de Industria, Turismo y Comercio, encargado de velar por la ciberseguridad de las PYMES y los ciudadanos en el ámbito doméstico.
- El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional, responsables de combatir la ciberdelincuencia.
- La Agencia Española de Protección de Datos, dependiente del Ministerio de Justicia, así como las Agencias de Protección de Datos de la Comunidad de Madrid y de la Generalitat de Cataluña.

Las principales empresas españolas del sector de la seguridad informática crearon, el año 2009, el Consejo Nacional Consultor sobre CiberSeguridad (CNCCS) con el objetivo de fomentar la defensa del ciberespacio y colaborar con las entidades públicas y privadas. Este organismo supone un avance significativo para la Ciberseguridad Nacional al estar respaldado por la iniciativa privada y facilitar normativas, asesoramiento,… a las empresas y en particular a sus departamentos de Seguridad Informática.

Entre los organismos internacionales europeos es de destacar la agencia europea ENISA (European Network Information Security Agency) cuya última iniciativa Cyber Europe 2010 hemos comentado anteriormente.

EL ESTADO ACTUAL DE LA CIBERSEGURIDAD DESDE LA PERSPECTIVA DE ORGANIZACIONES Y EMPRESAS

Cisco, la empresa norteamericana líder en el mundo de las comunicaciones y cada día más con intereses en muchas otras áreas como la seguridad, *cloud computing*, virtualización, en su informe *2010 Midyear Security* analiza cómo las grandes transformaciones tecnológicas, económicas y demográficas –la proliferación de dispositivos móviles conectados a la Red (teléfonos inteligentes, tabletas tipo iPad, etc.)

Hoy día y los próximos años, posiblemente lo confirmarán, nos encontramos con la implantación creciente del Internet móvil y la consiguiente proliferación de dispositivos móviles (acceso mediante todo tipo de dispositivos, teléfonos inteligentes, tabletas tipo ipad, libros electrónicos, microordenadores *netbooks*, ordenadores think (tontos, con poca memoria y capacidad de proceso conectados a *La Nube*) videoconsolas, acceso desde todo tipo de medios de comunicación, automóviles, trenes, aviones, autobuses, barcos, …), de las tecnologías *cloud computing,* la virtualización, o el avance imparable de las redes sociales y de los restantes medios sociales como *blogs, wikis, mashups* (de modo autónomo o integrados en redes sociales). Todo esto unido a la difusión también cada día mayor de las nuevas tecnologías en torno a la Geolocalización, Realidad Aumentada, la Web en tiempo real o el Internet de las cosas (acceso a la Red mediante todo tipo de «cosas», sensores, electrodomésticos, herramientas tecnológicas, etc. además de las mencionadas en los párrafos anteriores) están configurando grandes cambios sociales que afectarán significativamente a la capacidad de los departamentos de TI para mantener la seguridad de la Red.

Si nos centramos en las organizaciones y empresas, la imagen clásica del puesto de trabajo está variando completamente. Los trabajadores escriben en los ordenadores portátiles que se llevan a casa, escriben, ver la prensa o consultan sitios relacionados con el trabajo en los teléfonos móviles, iPhone, Blackberry, Android o el último recién llegado Windows Phone 7, realizan llamadas privadas y profesionales desde los mismos dispositivos anteriores. En el estudio de Cisco, la empresa nº 1 a nivel mundial en el mundo de las comunicaciones, que mencionamos anteriormente, *2010 Midyear Security,* un gran número de empresas consultadas reconocen que sus trabajadores han otorgado accesos no autorizados a familiares o amigos, y la mayoría no renuncia a acceder a redes sociales desde su puesto de trabajo. Otro dato ilustrativo es el caso omiso de los trabajadores a las

políticas corporativas, cita, p.e., el informe que el 50% de los usuarios finales ha admitido ignorar las políticas corporativas que prohíben el uso extensivo de redes sociales, mientras que un 27% reconoce haber cambiado la configuración de su equipo para acceder a aplicaciones no permitidas.

El estudio de Cisco está segmentado por áreas que pasamos a detallar así como las posibles soluciones que ofrece a cada uno de los riesgos y amenazas para la ciberseguridad el comportamiento dentro de las organizaciones y empresas, especialmente por parte de sus trabajadores. Una de las áreas de interés lo constituyen las transformaciones tecnológicas y sociales. Las transformaciones clave más importantes en los departamentos de organizaciones y empresas y que afecta sensiblemente a la ciberseguridad son: las redes sociales, la virtualización, la tecnología *cloud computing* y la apuesta creciente por integrar múltiples dispositivos móviles Para responder con éxito a estas transformaciones, Cisco propone que las empresas deberían:

- Aplicar políticas específicas para cada usuario en el acceso a las aplicaciones y los datos sobre sistemas virtualizados.
- Establecer límites estrictos en el acceso a la información crítica para el negocio.
- Crear una política corporativa oficial de movilidad.
- Invertir en herramientas para gestionar y monitorizar las actividades «en la nube».
- Proporcionar a los trabajadores guías sobre el uso de los medios sociales en la oficina.

Los cibercriminales están aprovechándose de las innovaciones tecnológicas para agilizar sus propias operaciones y obtener rentabilidad. «El cibercrimen cibernético es un negocio puro y duro. Nosotros (Cisco) vemos la seguridad desde el punto de vista de los atacantes, que se organizan como empresas. No siempre los fraudes más llamativos son los más rentables. Al revés, suelen serlo, los que requieren menos inversión» (PASCUAL 2010) (28). Por esta razón, Cisco ha elaborado una matriz de rentabilidad de los virus, de modo que muchos de los fraudes clásicos, incluso el phishing están dando paso a importar cuotas de alta en todo tipo de negocios, administraciones, etc. donde se roban pequeñas cantidades de dinero cada vez y se requiere poca inversión, este tipo de fraude requiere ingeniería social (formularios, llamadas no solicitadas, etc.).

(28) Declaraciones ya citadas de Pilar Santamaría, en *Cinco Días*, 10 de noviembre de 2010, p.14.

La matriz de Cisco considera muy rentables para el ciberdelincuente el fraude por clics, el farmacéutico y los ataques que se disfrazan de antivirus, los timos lucrativos,… Posteriormente volveremos en el capítulo 3 y con más detalle sobre la tipificación del crimen organizado.

Los cibercriminales están aprovechándose de las innovaciones tecnológicas para agilizar sus propias operaciones delictivas; por ejemplo, el estudio también destaca el uso creciente de las redes sociales y como los terroristas se están sumando a dichas redes sociales que se han convertido en terreno de juego para los cibercriminales con un creciente número de ataques. En este caso se ha desvelado que cada vez más usuarios dedican una mayor cantidad de su tiempo de trabajo en acceder a los juegos de las redes sociales, p. e. *Farmville* de Facebook. Aunque aparentemente solo se produce pérdida de productividad, en las horas de trabajo y no suponen una amenaza potencial, sin embargo los cibercriminales y cada día más los terroristas diseñan y construyen aplicaciones para propagar malware a través de estos juegos y lanzar las correspondientes amenazas.

En cuanto al futuro de las amenazas, el estudio de Cisco reseña también que la ingeniería social y la mezcla de tecnologías por parte de los usuarios son cada vez más peligrosas para la ciberseguridad. Está cada vez más al alza los ataques multivector que combinan diferentes soportes (correo-e, web, voz, vídeo,..) para encontrar fisuras. Los cibercriminales y, por ende, los ciberterroristas siguen atacando sitios web legítimos de forma planificada, a la vez que gestionan ataques de *spam* (29) controlados (ataques multivectoriales) preparados para actuar en un momento concreto y enfocados en establecer *keyloggers* (programas capturadores de teclado), *bots* y puertas traseras. La mezcla de tecnologías dirigidas a un solo objetivo es cada vez más frecuente; p.e. los cibercriminales intentan ganarse nuestra confianza con archivos audiovisuales que se prevén acapararán el 90% del tráfico en los próximos dos años (30).

Otros datos de interés para la ciberseguridad que aporta el estudio de Cisco es la constatación de que un porcentaje notable de los res-

(29) El estudio de Cisco reconoce que el *spam* sigue creciendo exponencialmente, a pesar del reciente descenso en operaciones criminales basadas en *spam*; se espera que durante 2010 crezca a escala mundial un 30% según destaca el informe complementario *Cisco Security Intelligence Operations.* Estados Unidos sigue siendo el país donde se origina más spam seguido por India, Brasil, Rusia y Corea del Sur.

(30) *Ibíd.*, p. 14.

ponsables de seguridad de las 500 empresas consultadas, consideran que los usuarios no autorizados son la principal amenaza a la seguridad corporativa, unida a las redes sociales y las nuevas aplicaciones que también se identifican como amenazas importantes. El informe es concluyente «las brechas de seguridad abiertas por esta nueva realidad son enormes. Los *hackers* lo saben y se aprovechan de ello».

Queremos resaltar y para concluir, de nuevo, para terminar las citadas declaraciones de Pilar Santamaría a *Cinco Días* «*en cuanto a que tanto las transformaciones tecnológicas como los nuevos modelos económicos y sociales repercuten directamente en la seguridad corporativa. Así, las empresas deben adaptarse hoy a estos cambios transformando su modelo de TI para poder responder con celeridad a las nuevas amenazas y conseguir una verdadera red sin fronteras*» (31).

II PARTE. Retos, Amenazas y Oportunidades de la Ciberseguridad

LOS OBJETIVOS DE LA OBRA

La obra que presentamos ha pretendido analizar el panorama actual del ciberespacio y como hacer frente a las amenazas que plantea sobre todo con el creciente uso de Internet, tanto tradicional como móvil, en organizaciones, empresas y ciudadanos en general, y, lógicamente a la Seguridad Nacional. Es preciso hacer frente a esas amenazas mediante las oportunas estrategias de seguridad, en nuestro caso, denominada ciberseguridad y en consecuencia la necesidad de una oportuna estrategia de ciberseguridad, y, por ende, la necesidad de diseñar y construir dicha estrategia en la Seguridad Nacional, pero que no debe restringirse sólo a las Administraciones públicas –nacional, autonómica y local– y a las Fuerzas Armadas sino que, naturalmente, debe llegar a las Infraestructuras Críticas, organizaciones y empresas de todo tipo, la industria y a los ciudadanos y claro es a la Sociedad española.

Sin embargo, la Ciberseguridad debe plantearse no sólo desde el punto de vista de las amenazas sino también desde los retos que plantean. La implantación de políticas de ciberseguridad servirá no sólo para la Seguridad Nacional sino también para aumentar la eficiencia y renta-

(31) Pilar Santamaría, Directora de Desarrollo de Negocio y Ciberseguridad de Cisco Mediterráneo, en declaraciones recogidas en un artículo de Manuel G. Pascual, en cinco Días, 10 de noviembre de 2010, p. 14.

bilidad de la industria y empresas del sector de la seguridad e incluso en una vertiente mucho más amplia de todos los sectores de la vida nacional que al tener aseguradas sus ciberdefensas podrán dedicarse, con tranquilidad, a sus negocios fundamentales (*core*) lo que redundará en el aumento de su productividad y beneficiará a sus empleados, clientes, socios, y, en general, a los grupos de interés (*stakeholders*).

El libro se ha organizado con un criterio académico, científico y de investigación, pero tratando que los estudios e investigaciones realizadas por los diferentes autores en sus respectivos capítulos, así como en la introducción y en las conclusiones, puedan ser de lectura asequible, no sólo a los expertos, interesados y aficionados en la ciberseguridad, sino también en todos aquellos lectores de otros sectores, interesados en conocer el impacto de la ciberseguridad en su vida diaria desde un aspecto positivo del término, aunque evidentemente se analizan situaciones de riesgo, ya pasadas, y las futuras que se puedan producir (32).

Pretende ser también una herramientas de consulta y análisis para estudiosos de universidades, profesores, investigadores, centros de investigación, empresas, órganos de pensamiento y opinión –al estilo de los *think tank* del mundo anglosajón–, … que deseen conocer las tecnologías más empleadas en el ámbito de la ciberseguridad empleadas en la Defensa Nacional, en áreas tales como Ciencias, Ingeniería, Derecho, Ciencias Sociales, Ciencias Económicas, Ciencias Políticas, Comunicación y Documentación y otros sectores afines, y la Sociedad en su sentido más amplio, dado el impacto que en ella producen.

EL CONTENIDO

En el Capítulo 1, se realiza un análisis generalista del alcance y ámbito de la Seguridad Nacional en el Ciberespacio. La autora especialista en Tecnologías de la Información tras examinar las definiciones usuales del ciberespacio y sus implicaciones, se introduce en la descripción y análisis de las consideraciones normativas y gestión de la seguridad en el ámbito español, europeo, norteamericano y OTAN. Como experta en el tema describe los tipos de ataques y de atacantes, cómo han evolucio-

(32) Debido a la visión de herramienta científica y de investigación del libro, se ha optado por incluir al principio de cada capítulo un Resumen (*Abstract*) y Palabras Clave (*Keywords*) al estilo tradicional de los artículos publicados en revistas científicas o en libros de actas de congresos.

nado los ciberataques y sobre todo las posibles y peligrosas amenazas a las Infraestructuras Críticas de interés nacional. Termina planteando desde la visión general que describe la necesidad de desarrollar unas estrategias de ciberseguridad.

En el capítulo 2, el autor divide su trabajo en tres partes clave para el contenido posterior del libro. 1. Expansión del Concepto de Seguridad nacional y la aparición de nuevos escenarios, amenazas y respuesta, que le llevan a considerar una descripción en profundidad del concepto de ciberseguridad y ciberamenazas, 2. Las respuestas del sistema legal donde analiza la situación legal a escala mundial, a nivel de la Unión Europea y la perspectiva dentro del Derecho Penal Español, que como experto internacional conoce muy bien y todo ello en un contexto de criminalidad organizada y terrorismo; 3. Termina con un balance necesario y de actualidad sobre el debate jurídico creado, analizando las categorías generales dl Derecho afectadas por los usos y abusos de las nuevas tecnologías y dedicando un apartado completo a resaltar las cuestiones más específicas de la creciente problemática surgida a raíz de los problemas generados por los usos y abusos citados.

El ciberespacio y el crimen organizado se describen en el capítulo 3 como una nueva realidad que ha dado origen al delito informático y la aparición del hacker, bien con el rol de persona romántica y altruista, normalmente, bien con el rol de pirata informático. Plantea el concepto *¿hacking by dólar*? para examinar una nueva figura «*comercial*» en la que el cibercrimen quiere conseguir rentabilidad económica apoyándose en la comisión de delitos informáticos (33). Por último describe y analiza la delincuencia organizada y los fraudes que originan tanto en el comercio electrónico como en la banca electrónica, sus dos grandes objetivos. El autor describe una figura emergente muy curiosa «Crime as a Service» en el que le asigna un modelo de servicio emulando a los modelos de entrega de servicios de la Computación en Nube (Cloud Computing); naturalmente está totalmente relacionada con la figura del hacking por negocios (por dólares) y «en esencia» sería como una correspondencia con los populares «Software as a Service» (SaaS) o «Infrastructure as a Service» (IaaS). También analiza el nuevo fenómeno de la infraestructura de las «mulas» como medio de transporte en la cadena del delito informático y la mutación del timo clásico en timo en la Red.

(33) Esta figura ha llevado a la multinacional Cisco en un informe publicado recientemente y ya analizado a elaborar un matriz de rentabilidad de los virus.

La Ciberseguridad es ya un tema de impacto global y por esta razón el capítulo 4 se dedica a analizar la situación en el marco internacional y dentro del mismo en la OTAN por su importancia para España como miembro activo de dicha organización internacional. El autor del capítulo, experto en Relaciones Internacionales nos plantea en primer lugar cual es la situación actual de la Ciberseguridad en el ámbito internacional. A continuación analiza con buen nivel de profundidad los dos casos más emblemáticos de la ciberguerra de gran impacto internacional y que llevaron a estados de todo el mundo a pensar en la necesaria protección antes amenazas cibernéticas. Estos casos han sido los conocidos de Estonia 2007 y Georgia en 2008. En ambos casos se analiza con gran detalle, desde los antecedentes, cronología, a los ciberataques, tipos, objetivos y las respuestas dadas desde el punto de vista técnico, político y legal, y de informática forense. Por último, su experiencia profesional le lleva a examinar la ciberseguridad en la OTAN, cómo se ha planteado y cómo se está haciendo y cómo se está haciendo frente en cumplimiento de los artículos 4, 5 y 6 del Tratado de Washington.

Naturalmente, una obra sobre Ciberseguridad no se podría proyectar sin analizar específicamente la ciberseguridad en el ámbito militar. Por esta razón el capítulo 5 se dedica a su estudio. El la autor comienza su trabajo con una larga introducción, necesaria, por otra parte, para situarse en el contexto del ámbito militar, haciendo una revisión general de las operaciones cibernéticas en redes y en la OTAN y citando, brevemente, por su interconexión, los ataques e incidentes en Estonia –ya tratado con profundidad, anteriormente en un capítulo anterior– y en Estados Unidos. En la segunda parte de su trabajo, el autor plantea ya la organización de la Seguridad de la Información y su normativa en el Ministerio español de Defensa, analizando el Plan Director CIS, la cooperación internacional, así como el plan de formación y adiestramiento de su personal, terminando con una necesaria reseña sobre el cifrado y *encriptación* en el ámbito militar.

El último capítulo se dedica lógicamente al análisis y planteamiento de las estrategias nacionales de ciberseguridad y al ciberterrorismo. El capítulo 6 comienza con la identificación de los agentes de la amenaza (ciberterrorismo y ciberespionaje) para continuar con el análisis de las infraestructuras críticas y su rol en la Defensa Nacional, describiendo su catálogo, el Plan de Protección y posibles ataques, en particular, a sistemas SCADA. A continuación se describen las estrategias nacionales de ciberseguridad en diferentes países y en organizaciones internacionales. Una vez realizado el análisis internacional se centra en España y en los

diferentes Ministerios con competencias en temas de ciberseguridad, así como la situación actual de España, analizando los ámbitos de actuación, sistemas clasificados, el Esquema Nacional de Seguridad, la situación de la protección de datos personales y se completa el capítulo con los objetivos y las líneas estratégicas de acción de la Estrategia Española de Ciberseguridad junto con una posible estructura de la ciberseguridad.

En las conclusiones se recogen una síntesis de las conclusiones parciales de los diferentes autores de los capítulos, así como de esta Introducción, a modo de recomendaciones prácticas para una futura estrategia nacional de ciberseguridad, pero resaltando que es de gran importancia, por su impacto en la Defensa Nacional, que las estrategias de ciberseguridad deben contemplar una coordinación general no sólo de la ciberdefensa en las Administraciones Públicas sino también del catálogo de Infraestructuras Críticas, de organizaciones, empresas, industrias, centros científicos y de investigación y también de los ciudadanos, ya que dado que el acceso a Internet, fijo y móvil, entendemos, deberá ser declarado un derecho fundamental, en muy poco tiempo toda la población española deberá tener acceso a la Red como tiene derecho a cualquier otro de los servicios de interés general como la luz, el agua, el teléfono o la electricidad.

Por último destacar que este Cuaderno de Ciberseguridad del Instituto Español de Estudios Estratégico refleja la opinión de los siete autores sobre la Ciberseguridad en España y su interrelación con el ámbito internacional y se encuentra enmarcado dentro de los objetivos del Instituto y, en particular, en el área del Ciberespacio y la Ciberseguridad del mismo. Ha pretendido mostrar el Estado del Arte de la Ciberseguridad a nivel internacional pero lógicamente se ha centrado en España y en los Organismos Internacionales a los que pertenecemos. El libro busca también mostrar la necesidad de una estrategia de ciberseguridad a nivel nacional pero ofreciendo también, a la vez, los retos y oportunidades que un buen plan director de ciberseguridad tendrá en el desarrollo futuro de todo tipo de organizaciones y empresas, en la industria y en los negocios, y en los ciudadanos que, por ende, constituyen la actual y futura Sociedad Española.

BIBLIOGRAFÍA

CARR Jeffrey. *Cyber Warfare*. Sebastopol, USA, O´Reilly, 2010.

CLARKE Richard y KNAKE Robert K. *Cyber War: The Next Threat to National Security and What to Do About It,* New York, Harper Collins, 2010.

Federal Government USA. *Cyberspace Policy Review*. [en línea] www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

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

KRUTZ Ronald y DEAN Vines Russell. *Cloud Security. A Comprehensive Guide to Secure Cloud Computing*, Indianapolis, Wiley, 2010.

LIBICKI Martin C. *Cyberdeterrence and Cyberwar*, Santa Mónica, RAND Corporation, 2009.

LYNS III William J, «Defending a New Domain: The Pentagon's Cyberstrategy», *Foreign Affairs*, vol. 89, nº 5, septiembre/octubre de 2010, pp. 97-103. [en línea] www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

PASCUAL Manuel, Entrevista a Pilar Santamaría de CISCO en *Cinco Días*, 10 de noviembre, 2010, p.14.

The Economist. «Cyberwar. The thread from the Internet», Volumen 396, número 8689, 3-9 de julio de 2010.

Referencias Web de Ciberseguridad

- Draft National Strategy for Trusted Identities in Cyberspace www.nstic.ideascale.com/
- The Comprehensive National Cybersecurity Initiative www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
- The Cyberspace Policy Review (pdf) www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- The Cyberspace Policy Review supporting documents www.whitehouse.gov/cyberreview/documents
- The National Initiative for Cybersecurity Education (pdf) www.whitehouse.gov/sites/default/files/rss_viewer/cybersecurity_niceeducation.pdf
- Cybersecurity R&D
- cybersecurity.nitrd.gov/