MINISTERIO DE DEFENSA

CUADERNOS de ESTRATEGIA

149

CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS
INSTITUTO UNIVERSITARIO «GENERAL GUTIÉRREZ MELLADO»

MINISTERIO DE DEFENSA

CUADERNOS de ESTRATEGIA

149

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS
INSTITUTO UNIVERSITARIO «GENERAL GUTIÉRREZ MELLADO»

CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

Diciembre 2010

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
http://www.publicacionesoficiales.boe.es

Edita:

MINISTERIO DE DEFENSA
DIRECCIÓN GENERAL DE RELACIONES INSTITUCIONALES

NIPO: 075-11-012-0 (edición en papel)
ISBN: 978-84-9781-622-9
Depósito Legal: M-3045-2011
Imprime: Imprenta del Ministerio de Defensa
Tirada: 1.000 ejemplares
Fecha de edición: febrero 2011

NIPO: 075-11-013-6 (edición en línea)

administración electrónica

En esta edición se ha utilizado papel libre de cloro obtenido a partir de bosques gestionados de forma sostenible certificada.

DIRECCIÓN GENERAL DE RELACIONES INSTITUCIONALES
Instituto Español de Estudios Estratégicos

Grupo de Trabajo número 03/10

CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

SUMARIO

PRESENTACIÓN

En el reciente Concepto Estratégico de la OTAN aprobado en la Cumbre de Lisboa, los ciberataques se consideran uno de los principales riesgos. En el llamado Informe Solana de diciembre de 2008, a los cinco años de la aprobación de la Política Europea de Seguridad y Defensa (PESD) de la Unión Europea, también se consideró necesario incluir esta amenaza entre las principales a tener en cuenta. Parecía pues, oportuno elaborar un cuaderno de estrategia sobre lo que sin duda, es uno de las principales preocupaciones de seguridad de los países más desarrollados y de las organizaciones internacionales como la OTAN y la UE.

El tema tratado es un tema poliédrico con múltiples aspectos a considerar. En este cuaderno hemos renunciado a contemplar todos los aspectos pero hemos procurado abordar los más importantes desde el ámbito de seguridad y defensa, para ello, hemos reunido a seis ponentes expertos en diferentes áreas que bajo la batuta del catedrático Luis Joyanes Aguilar han realizado una excelente obra que aquí presentamos.

Miguel Requena y Díez de Revenga
Director
Instituto Universitario General Gutiérrez Mellado

Miguel Ángel Ballesteros Martín
General Director
Instituto Español de Estudios Estratégicos

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/

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.

CAPÍTULO SEGUNDO

ESTRATEGIAS LEGALES FRENTE A LAS CIBERAMENAZAS

ESTRATEGIAS LEGALES FRENTE A LAS CIBERAMENAZAS*

JOSÉ L. GONZÁLEZ CUSSAC

**El presente trabajo se inserta en el marco del Proyecto de investigación «Nuevas amenazas a la seguridad nacional: terrorismo, criminalidad organizada y tecnologías de la información y la comunicación» (Ministerio de Ciencia e Innovación, referencia DER2008-05707).*

RESUMEN

Estrategias legales frente a las ciberamenazas

En el contexto socio-económico global actual, el desarrollo del ciberespacio ha facilitado enormemente el auge de toda clase de interacciones comerciales, sociales, gubernamentales y delictivas. Lo cual ha tenido como consecuencia que la seguridad del ciberespacio haya crecido en importancia, desde el momento en que las ciberamenazas han pasado a formar parte esencial de las nuevas agendas de seguridad nacional y defensa. Así, los países han dedicado parte de sus esfuerzos, en los últimos años, a desarrollar una estrategia legal que pueda ser efectiva para seguir el rastro de las ciberamenazas y contraatacarlas, y, al mismo tiempo, sea respetuosa con los derechos y libertades fundamentales.

Precisamente en ese ámbito se enmarca este trabajo, que encuentra su principal objetivo en el intento de ofrecer un panorama descriptivo de la evolución de las diferentes respuestas legales dadas a las ciberamenazas. En particular, el trabajo analiza sucintamente las medidas penales adoptadas para hacer frente a los cibercrímenes. Y concluye aportando algunas consideraciones críticas sobre la aproximación realizada hasta el momento a este tema.

Palabras clave: Ciberamenazas, Ciberseguridad, Cibercrimen, Medidas legales, Jurisdicción, Derecho Internacional, Internet, Globalización.

ABSTRACT

«Legal Strategies against Cyber Threats»

In the world's current global socio-economic context, the rise of cyberspace has greatly facilitated all kinds of commercial, social governmental and criminal interaction. As a result, the security of cyberspace has grown in importance, from the moment that cyber threats have become an essential part of the new agendas for national security and defense. So the countries have devoted part of its efforts, in recent years, to develop a legal strategy that can be effective to track and counteract cyber threats, but still mindful of fundamental rights.

Precisely, that is why the principal mission of this research, will be to study the development of the different legal responses into the cyber threats. Particularly, the research provides a brief analysis of the criminal measures adopted against the cybercrimes. It also concludes offering some critical considerations of this issue.

Keywords: Cyber threats, Cybersecurity, Cybercrime, Law Enforcements, Jurisdiction, International Law, Internet, Globalization.

EL PUNTO DE PARTIDA. LA EXPANSIÓN DEL CONCEPTO DE SEGURIDAD NACIONAL: *CIBERDELITOS Y CIBERAMENAZAS*

La expansión del concepto de seguridad nacional

Para poder comprender la función del Derecho –en particular del derecho penal– frente a las nuevas amenazas, y en concreto frente a las llamadas *ciberamenzas*, resulta preciso destacar algunos parámetros que están experimentando una profunda y constante transformación.

Comenzaré por la mutación expansiva de la categoría jurídica de seguridad nacional, que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta uno propio de seguridad nacional. Si bien es cierto, que éste no ha acabado de perfilarse con la suficiente concreción jurídica, discurriendo en numerosas ocasiones entre su entendimiento como idea simbólica-emotiva, o como equivalente a interés general identificado con el interés del Estado y contrapuesto al interés individual. De aquí el usual manejo

del canon de ponderación de intereses para resolver los conflictos entre seguridad nacional y derechos fundamentales (1).

Es precisamente en este contexto donde se manifiesta nítidamente la necesaria reconstrucción del concepto de seguridad nacional, para, de una parte, que resulte eficaz como criterio central de gestión de las nuevas amenazas y necesidades estratégicas actuales, y de otra, cohonestarla con nuestra forma de organizarnos políticamente: el Estado democrático y de Derecho.

Pues bien, en el transcurso de este proceso, parece claro que la categoría de seguridad nacional se construye ya hoy desde una perspectiva multidimensional: militar, política, económica, social (identitaria), y medioambiental. Es decir, como equivalente a exención de peligro, daño o riesgo en todos estos ámbitos, y por tanto entendida como seguridad colectiva, compartida y global.

Como es conocido, esta necesaria adaptación conceptual de la seguridad nacional se debe a múltiples factores: cambios en el sistema internacional; avances en la tecnología de la información, comunicación y transporte; aparición de amenazas post-guerra fría; reactivación de conflictos étnico-religiosos; estallido de crisis económico-financiera; resurgimiento de la competitividad geopolítica; mantenimiento o rebrote de conflictos locales; aparición de nuevos actores no estatales; facilidad con que grupos no estatales se organicen para atacar Estados utilizando nuevas tecnologías; etc.

Así pues, creo que resulta innecesario insistir en aspectos obvios acerca de los grandes cambios sufridos, y en curso, del mundo actual. Pero sí referirme, muy sucintamente –pues también constituyen ya lugares comunes en la literatura especializada–, a los presupuestos básicos desde los que arrancan estas reflexiones. En concreto, deseo partir de la nueva consideración que las instituciones y organismos competentes en materia de seguridad proyectan ahora sobre algunos fenómenos que tradicionalmente preocupaban en otras áreas sociales, y algunos casi exclusivamente en la esfera de la administración de justicia (derecho penal).

Para ilustrar esta tendencia, basta con citar, a título de ejemplo, entre otros muchos posibles, el documento la Estrategia Europea de Seguri-

(1) GONZÁLEZ CUSSAC, J. L.: «*Nuevas amenazas a la seguridad nacional: el desafío del nuevo terrorismo*», en «Retos de la política criminal actual», Revista Galega de Seguridade Pública (REGASP)«, nº 9, Xunta de Galicia, 2007, p. 233 a 252

dad, de diciembre de 2003 y el Informe del Parlamento Europeo sobre su aplicación (2009/2198/INI). En el primer texto se indica que «*la unión de diferentes riesgos y amenazas, como son el terrorismo empeñado en ejercer la máxima violencia, la disponibilidad de armas de destrucción masiva, la delincuencia organizada, el debilitamiento del sistema estatal y la privatización de la fuerza, constituyen una amenaza muy radical*» (2).

Como se observa, viejos fenómenos de delincuencia común, en particular terrorismo y criminalidad organizada, han pasado de ser considerados como simples «riesgos» a la seguridad nacional, hasta alcanzar la máxima categoría de «amenaza». Así pues, se encuentran al mismo nivel que los eventuales ataques de fuerzas armadas de países hostiles. Todos los documentos nacionales o internacionales sobre estrategia y seguridad así lo confirman. Por consiguiente, estos fenómenos, especialmente terrorismo y crimen organizado, ya no se abordan como una cuestión meramente criminal, sino que se afrontan también desde otras perspectivas, y desde luego comportan otras muchas proyecciones que la vieja delincuencia raramente tuvo. Todo ello conlleva muchos cambios y sobre todo abre numerosos interrogantes.

Un ejemplo es suficiente para subrayar la incidencia de estas novedosas proyecciones del terrorismo y del crimen organizado sobre las agendas de seguridad nacional: la globalización, la *deslocalización,* la ausencia de fronteras y las dificultades para identificar al atacante y capturarlo. Esta es sin duda una de las cuestiones claves a resolver por los sistemas legales en la actualidad: ¿cómo hacer frente jurídicamente a un delincuente del que no se conoce exactamente ni su identidad ni su ubicación espacial? Es evidente que las estrategias de la disuasión ya no son suficientes, ni en el terreno militar ni tampoco aparentemente en el jurídico.

Entonces, la primera consideración básica sería la siguiente: aunque hasta ahora las fuerzas armadas protagonizaban la defensa de nuestra seguridad nacional, en la actualidad, ante la diversificación de las amenazas, ya no son el aparato estatal exclusivo encargado para garantizar

(2) Ver ARTEAGA: «La estrategia europea de seguridad: cinco años después», ARI nº 15/2009, Real Instituto Elcano, 22/01/2009; Informe del Parlamento Europeo de 2 de marzo de 2010 www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2010-0026+0+DOC+XML+V0//ES, y, SHULMAN: «Medidas del Consejo de Europa para luchar contra la cibercriminalidad», en ENAC, nº 2, agosto 2009, pág. 31.

nuestra supervivencia (3). Pero a la vez, en paralelo, tampoco parece hoy posible convenir que la administración de justicia sea una herramienta suficiente para resolver los conflictos atinentes a crimen organizado y terrorismo. La premisa puede formularse con otras palabras: si en realidad lo que está en peligro es nuestro sistema de convivencia, nuestra seguridad nacional, en este marco el Derecho, la administración de justicia, y en particular el derecho penal, tampoco resulta ser el instrumento idóneo, suficiente o único para enfrentarse a estas amenazas.

En resumen, hoy parece una evidencia comúnmente aceptada que nos hallamos ante un nuevo escenario estratégico, criminológico y político-criminal, en el que se aprecia no sólo un salto cuantitativo sino cualitativo. Y en este sentido se habla de una ruptura: los escenarios de ataques son muy variados, con diferentes niveles de riesgo y de muy diversa escala de impacto potencial, lo que complica extraordinariamente su prevención y respuesta estatal. Ahora el *nuevo terrorismo y la nueva criminalidad transnacional*, se muestran con una mayor agresividad y representan un auténtico desafío para los Estados. Pero su control igualmente hace peligrar los valores del Estado de Derecho, especialmente la de los derechos fundamentales. Expresado en otros términos, la amenaza real de estas formas de criminalidad provocan una demanda apropiada de la respuesta estatal y con ello también se realimenta el viejo debate entre seguridad y libertad.

Nuevos escenarios, nuevas amenazas, nuevas respuestas

El desarrollo del ciberespacio ha facilitado enormemente el desarrollo de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales. Hoy en día se ha encaminado el control de muchos procesos mundiales a través del ciberespacio. Por lo que no hay duda de que actualmente el ciberespacio constituye un bien valioso. Y de que la seguridad del ciberespacio ha crecido en importancia (4).

En efecto, porque si combinamos estas reflexiones con el fenómeno de las *ciberamenazas*, constatamos como la criminalidad organizada en general y el terrorismo en particular, están generalizando el uso de las nuevas tecnologías de la información y la comunicación como instrumen-

(3) BALLESTEROS MARTÍN, M. A.: «*El papel de las fuerzas armadas en la lucha contra el terrorismo internacional*», en Real Instituto Elcano de Estudios Internacionales y Estratégicos, 18/08/2006.

(4) YAR: «Cybercrime and society», London 2006.

to para desarrollar su actuación delictiva. Sin embargo, la novedad de esta circunstancia no es tanto el uso delictivo de las mismas, sino que su empleo sofisticado y masivo en un escenario global, hasta el momento no ha encontrado una respuesta adecuada y satisfactoria ni en el sistema legal ni en el de la cooperación de las diferentes agencias de seguridad.

Sin duda alguna, durante el control de Al Qaeda en Afganistán, se desarrolló una auténtica academia de ciberterrorismo con el objetivo de buscar formas de atacar las infraestructuras occidentales en el ciberespacio. Aunque no hay que dejar de recordar que parte de la complejidad en este análisis, surge del hecho de que los diferentes Estados experimentan las ciberamenazas de manera diferente, lo cual hace que resulte una asimetría en la preocupación acerca de las mismas.

Las posibilidades de globalización e internacionalización que tales tecnologías ofrecen, junto con las indudables ventajas que supone el llevar a cabo actuaciones que pueden producir sus efectos incluso en otro continente, convierte a estas categorías criminógenas en aún más peligrosas y efectivas de lo que hasta el momento venían siéndolo, y en cierta manera generan un clima de miedo, inseguridad e impunidad, unas veces real y otras distorsionado. Tales circunstancias obligan a desarrollar un análisis detenido de los ordenamientos jurídicos nacionales y de la normativa internacional, a efectos de determinar las carencias de las que adolecen, y así posibilitar un debate serio y riguroso de reformas jurídicas tendentes a aumentar la eficacia de la respuesta jurídica, que suplan las deficiencias actuales (5).

Probablemente, si hubiera que escoger una característica que definiera al siglo XXI, ésta sería, sin duda alguna, la globalización. En efecto, la disolución de las fronteras, el establecimiento de espacios comunes, cada vez de mayor amplitud, no sólo en el aspecto económico y social, sino también en el político y en el jurídico, están posibilitando espacios de actuación en continuo incremento. Como es sabido, esta realidad también provoca efectos negativos, y en nuestra temática se plasma en la generación de un idéntico proceso de internacionalización y expansión de la criminalidad.

Como se ha destacado sobradamente, en este contexto, las grandes amenazas que en el presente se ciernen sobre la seguridad pública y

(5) ROMEO CASABONA (coord.): «*El Cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas políticocriminales*», Granada 2006.

la seguridad nacional vienen determinadas por la criminalidad organizada y por el terrorismo. Dejando al margen las estrategias de naturaleza militar, tradicionalmente más propias de enfrentamientos armados entre Estados, en su condición de sujetos activos de Derecho internacional, la consideración de estos fenómenos como conductas delictivas, tanto en convenios internacionales como a nivel nacional, genera el que los métodos de prevención y represión en relación a ambos –particularmente complejo es el caso del terrorismo–, hayan de revestir una respuesta combinada y coordinada de la administración de justicia y de las fuerzas armadas (6). No obstante, en estas líneas el enfoque dominante es el análisis de las estrategias legales, esto es, de carácter jurídico y no tanto militar. A reforzar las mismas debiera dirigirse la labor de los poderes públicos y también de la literatura científica, posibilitando una auténtica cultura de seguridad nacional, en la que junto a la defensa de nuestra supervivencia física (*lo que somos),* se articulara la defensa de nuestros valores democráticos *(como somos)* (7).

Si a dicha profesionalización, internacionalización y globalización de la criminalidad acabada de referir, añadimos la consolidación del uso de las tecnologías de la información y la comunicación (TIC), obtenemos los ejes esenciales que configuran la realidad sobre la que gira este trabajo. En este sentido, en sí mismas las TIC constituyen instrumentos de alto valor patrimonial, político y estratégico; pero tampoco deben minusvalorarse las facilidades que el uso de las nuevas tecnologías ofrece para la ejecución de ilícitos, lo que a su vez conlleva la generalización y aumento del recurso a estas tecnologías como instrumento comisivo: el activismo, el hacktivismo y el terrorismo informático son algunos ejemplos claros de esta tendencia.

Quizás por este doble sentido de las TIC, como valor intrínseco y como instrumentos comisivos, la literatura jurídica ya comenzó a diferenciar, en la década de los ochenta, entre la criminalidad informática, consistente en la realización de determinados delitos que sólo pueden materializarse a través de mecanismos informáticos o sobre los mismos programas y sistemas informáticos; y la criminalidad clásica relacionada con la informática, relativa a las figuras delictivas tradicionalmente con-

(6) CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010.

(7) FERNÁNDEZ RODRÍGUEZ y SANSÓ-RUBERT PASCUAL (editores): «Internet: un nuevo horizonte para la seguridad y la defensa» (Seminario de Estudios de Seguridad y Defensa de la USC-CESEDEN). Universidad de Santiago de Compostela 2010.

tenidas en los textos punitivos en los que la presencia de estas tecnologías no es sustancial a las mismas, sino instrumental (8).

Ciberdelitos y ciberamenazas

Como hipótesis, podría decirse que cibercrimen y ciberamenazas no son categorías equivalentes, pues existen ciberdelitos que no constituyen amenazas a la seguridad nacional, ni todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética. Ahora bien, en los supuestos mencionados, determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional.

Para mostrar la diferente escala de gravedad que pueden revestir estas conductas, me valdré de algunos ejemplos. Con ello quiero significar que la respuesta debe distinguir igualmente la magnitud de la agresión, y no solo para ser proporcional, sino también para ser eficaz.

El actual concepto de *ciberespacio*, «como conjunto de medios y procedimientos basados en las TIC y configurados para la prestación de servicios», nos ofrece un primer criterio para discernir las diferentes entidades de las posibles agresiones y por consiguiente, de las necesidades de regulación jurídica. Hasta fechas recientes, la *ciberseguridad* respondía a la exigencia de tutelar la información (*Information Security)*, lo que determinaba un enfoque legislativo destinado a sancionar los accesos, usos, revelaciones, o daños ilícitos no autorizados. Sin embargo, en la actualidad, la evolución conduce hacia la gestión de riesgos del ciberespacio (*Information Assurance)*, en la que los riesgos para la seguridad se encuentran vinculados al uso, procesamiento, almacenamiento y transmisión de información o datos, y los sistemas y procesos utilizados. Hoy la *ciberseguridad* requiere de ambos enfoques, diferentes pero complementarios (9).

La importancia de la seguridad en el ciberespacio ha llevado a los principales países a desarrollar estrategias, planes y legislación tendente a prevenir y sancionar conductas delictivas, pero también a neutralizar ciberataques a su seguridad nacional –se habla de un hipotético «ci-

(8) FREUND, W., *Die Strafbarkeit von Internetdelikten*, Wien, 1998; GÜNTER, R., *Computer criminalität*, bhv, 1998

(9) FOJÓN CHAMORRO Y SANZ VILLALBA: «Ciberseguridad en España: una propuesta para su gestión», ARI 101/2010, Real Instituto Elcano 18/06/2010.

ber-11S» o de un «ciber-Katrina»– (10). Es más, en múltiples círculos se formulan listados de Estados hostiles en este ámbito. Así, por ejemplo, según la organización privada «Reporteros Sin Fronteras», en un informe de marzo de 2009, se identifica a los 12 «enemigos de Internet»: Irán, China, Cuba, Egipto, Corea del Norte, Siria, Túnez, Arabia Saudí, Vietnam, Myanmar, Turkmenistán y Uzbekistán.

Pues bien, determinados los objetos de tutela, procede identificar las amenazas a los mismos, que en todo caso son muy heterogéneas y presentan una naturaleza de alta innovación. Parece existir cierto acuerdo en clasificarlas, en consideración a su autoría e impacto, en las cuatro siguientes categorías:

A) Ataques perpetrados o patrocinados por Estados. Sería la traslación al ámbito virtual de los conflictos reales entre países. Los ataques a infraestructuras críticas o clasificadas o la denominada ciberguerra, constituyen buenos ejemplos.

B) Ataques cometidos por grupos terroristas o por cualquier otra manifestación de extremismos políticos, ideológicos o religiosos. Planificación de acciones y su ejecución, sabotajes, apología, captación o reclutamiento serían las principales conductas a considerar (11).

C) Los ataques de la delincuencia organizada. El anonimato y las fronteras nacionales ofrecen una alta rentabilidad para su uso en fraudes económicos a gran escala o explotaciones de redes de pornografía infantil.

D) Por último, se identifican los ataques de perfil bajo. Su naturaleza es muy heterogénea, incluyendo desde intromisiones en la intimidad hasta pequeños fraudes.

   Resulta fácil concluir que, dada la generalización del uso de las TIC, los ataques e intensidad de los mismos, son tan dispares que llegan incluso a difuminar los bienes a proteger. A título orientativo pueden citarse las siguientes modalidades de ataque: abusos en el acceso a correos e internet; accesos no autorizados; *bots* o redes de equipos infectados remotamente; captura de contraseñas; extorsiones debidas a informaciones; diversas clases de daños y sabotajes (v gr desfiguración de páginas web); múltiples varieda-

---

(10) Por ejemplo, consultar LEWIS, J.: «Security Cyberspace in the 44th Presidency», Report 2008; o Doctrina militar rusa y seguridad en la información: www.belt.es/expertos/HOME2_experto.asp?id=4999.

(11) CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010.

des de fraudes; *phishing*, consistente en el uso de redes sociales para adquirir de los usuarios información personal; denegación de servicio; infección por *malware* o uso de programas de códigos hostiles; *exploit*, consistente en la utilización de piezas, fragmentos o secuencias de datos o comandos para aprovechar fallos del sistema para lograr comportamientos no deseados en los programas; explotación de servidores y navegadores; hurtos y robos de ordenadores o dispositivos móviles; etc.(12).

E) Pero en todo caso, si hasta fechas muy recientes las empresas privadas eran las que lideraban los avances en ciberseguridad, ahora son los gobiernos los que han comenzado a protagonizar una enorme inversión en proteger el ciberespacio. Por eso mismo, son también muchos los Estados que ya consideran al mismo un activo de su seguridad nacional

Ciertamente en una primera fase los ataques en el ciberespacio fueron protagonizados por jóvenes que mostraban su destreza informática; pero después se profesionalizaron y comercializaron estas prácticas ilegales al descubrirse su rentabilidad, facilidad comisiva y considerable impunidad. En una tercera fase, su generalización ha despertado, como acabamos de señalar, el interés de los Estados ante la grave amenaza que suponen, a la vez que posibilitan nuevas formas de defensa y ataque. Algunas hipótesis ilustran perfectamente esta evolución: los posibles ataques a los sistemas que manejan las infraestructuras públicas, como los servicios de telecomunicaciones, de agua, luz, y gas, o los de transporte. En ocasiones el problema de su protección se complica al estar estos servicios prestados por empresas privadas.

También se afirma, en una reciente publicación (13), que el Pentágono sufre diariamente 5.000 ciberataques. Esta cifra puede resultar orientativa del volumen e intensidad del problema.

Y por otra parte, según fuentes gubernamentales norteamericanas, las pérdidas por fraude de datos y piratería en 2008, ascendieron a una cifra estimada de 720.000 millones de euros. Este dato es significativo del volumen económico del cibercrimen (14).

---

(12) PANSIERA, F. J., y JEZ, E., «La criminalité sur l'internet», Puf, 2000; PICCOTI, L., (Coord.), «Il diritto penale dell´informatica nell´epoca di internet», Padova, 2004.

(13) *Quadrennial Defense Review*, número de febrero de 2010

(14) Enlace web cybersecurity FBI www.fbi.gov/cyberinvest/cyberhome.htm

Un resumen de los incidentes más graves conocidos en los últimos años puede sernos de utilidad para tratar de comprender exactamente la dimensión del problema (15).

Abril-Junio 2007

- Una serie de ciberataques a agencias y departamentos del gobierno de los Estados Unidos acabaron con el robo de entre 10 y 20 terabytes de información. Entre las principales víctimas se encontraba el Secretario de Defensa, Robert Gates, cuya cuenta de correo electrónico no clasificada fue penetrada.

Mayo 2007

- El Parlamento, los Bancos, Ministerios y medios de comunicación de Estonia se enfrentaron a ataques distribuidos de denegación de servicio (denominados en inglés, DDoS – *Distributed Denial of Service*–). Son ataques a un sistema de computadoras *o de red*, que causan que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conexión a la red. En los ataques DDoS, los sitios web son inundados con un tráfico tal, que origina su colapso.

Octubre 2007

- Se envió un correo electrónico a 1000 miembros de la plantilla del *Oak Ridge National Labs*, del Departamento de Energía, de los USA, con un adjunto (attach) que contenía el acceso a las bases de datos no clasificadas de los Laboratorios.

Agosto 2008

- *Hackers* lograron introducir fotos de Hitler en la página oficial del Ministerio de Asuntos Exteriores de Georgia, al tiempo que otras páginas oficiales sufrían ataques distribuidos de denegación de servicio (DDoS). Algunos analistas norteamericanos concluyeron que el gobierno ruso estaba detrás de los ataques, y probablemente había actuado a través de los canales del crimen organizado.

(15) Center for Strategic and International Studies Technology and Public Policy Program. CSIS. Washington D.C. USA.

Agosto-Octubre 2008

- *Hackers* lograron el acceso a los correos electrónicos y archivos de los ordenadores de los cuarteles generales de Barack Obama y de John McCain, durante la campaña para las elecciones presidenciales.

Noviembre-Diciembre 2008

- Algunos miles de ordenadores militares en Tampa, en los cuarteles generales para operaciones militares entre el este de África y Asia central, son infectados con *software* dañino. Los investigadores concluyeron que el programa maligno fue introducido mediante *pen-drives* que habían sido dejados en una plaza de aparcamiento.

Marzo 2009

- Investigadores de la Universidad de Toronto anunciaron que habían descubierto una amplia red de ciberespionaje, que denominaron «GhostNet.». Los operadores de esta red infectaron 1.295 ordenadores principales en 103 países, de todo el mundo. Aunque no se ha podido determinar el origen de los operadores, diversos analistas apuntan a China.

Julio 2009

- Diversos ciberataques son lanzados contra las páginas web de los gobiernos, instituciones financieras y medios de Corea del Sur y los USA. Entre los objetivos estaba la página web del Washington Post (washingtonpost.com). Corea del Sur culpa a Corea del Norte de los ataques, pero la autoría no ha podido ser determinada todavía.

Diciembre 2009

- Google, y más de otras 30 empresas norteamericanas, instaladas en China, sufrieron ataques informáticos que ocasionaron, a muchas de ellas, la pérdida de secretos tecnológicos.

Con todo, hay que reconocer que los ciberataques están llegando a ser cada vez más sofisticados y, por tanto, más difíciles de rastrear. Se asegura que los *hackers* en China, por ejemplo, son ahora mismo capaces de tomar el control simultáneamente de miles de ordenadores per-

sonales en los USA, y, por control remoto, ordenarles el envío de correos electrónicos falsos o virus.

Hasta el día de hoy, la mayoría de los ataques informáticos se han recogido bajo la denominación de la categoría de «Cibercrimen». Ciertamente, todavía no ha habido actos realmente significativos de ciberterrorismo en los USA ni en ningún otro país, según los informes oficiales (16). Lo que se atribuye al hecho que *al Qaida* y otros grupos terroristas están todavía desarrollando sus ciber capacidades. Ahora bien, el desarrollo de las mismas en estos últimos años, sobre todo desde 2008, está siendo tan importante, que se prevé que en menos de 10 años esos grupos terroristas puedan estar ya plenamente preparados para lanzar sus principales atentados en el ciberespacio (17). En realidad, como acabamos de comprobar al exponer los casos más significativos, los ataques de referencia cometidos contra gobiernos extranjeros y corporaciones empresariales han sido, en gran medida, con fines de espionaje y fraude.

En resumen, mientras parece existir acuerdo en que Internet ha tenido un gran impacto sobre la criminalidad, en lo que no parece existir tanto consenso es en determinar sobre qué delitos en concreto ha recaído dicho impacto. Muchos autores afirman que prevalecen los cibercrímenes –esto es, los llevados a cabo a través de ordenadores en la red–, pero no hay, hoy por hoy, una definición común de lo que es cibercrimen ni, por ende, de los delitos que exactamente abarca (18).

No obstante, con carácter general, el concepto de cibercrimen abarca un conjunto de actividades ilícitas asociadas con el uso de TIC, especialmente en Internet. Actividades que pueden ir desde el fraude financiero hasta la entrada no autorizada a sitios web, e incidir en ámbitos como el espionaje industrial, la pornografía o los juegos de azar, entre otros. Así, entre algunos de los ciberdelitos más comunes se encuentran: el acceso ilegal a sistemas ajenos, la intercepción ilegal, la interferencia y pérdida de datos, la interferencia de sistemas, la pornografía infantil, los delitos

(16) TAIPALE, K. A.: «Seeking Symmetry on the Information Front Confronting Global Jihad on the Internet», National Strategy Forum Review, Vol. 16, summer 2007.

(17) CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010.

(18) WALL, D. S.: «The Internet as a Conduit for Criminal Activity», INFORMATION TECHNOLOGY AND THE CRIMINAL JUSTICE SYSTEM, Pattavina, A., ed. Sage Publications, Inc., 2005, pp. 77-98.

contra la propiedad intelectual, y el fraude electrónico. Sin embargo, por diversas insuficiencias en materia de legislación, su persecución tiene ciertas limitaciones. Todavía más confusa resulta la brecha existente entre los cientos de miles de incidentes ilegales estimados y el relativamente escaso número de procesos penales abiertos (19).

En el contexto descrito, algunos autores se plantean si los cibercrímenes son realmente una nueva categoría de delitos necesitada de una nueva teoría y clasificación, o si no estamos ante unos delitos que, sin necesidad de nuevas clasificaciones ni teorías, pueden ser entendidos desde las categorías delictivas clásicas ya existentes (20). Incluso los que van más allá, se plantean que la sensación de inseguridad en la red y de la alarmante existencia de cibercrímenes no es sino producto de recursos de información creados artificialmente por la propia industria de ciberseguridad que, sin duda, tiene interés en la dramatización de los cibercrímenes; esto es, en la creación de una sensación subjetiva de inseguridad y alarma en la red.

LAS RESPUESTAS DEL SISTEMA LEGAL

Pues bien, en todo caso, ambos fenómenos –*ciberdelitos y ciberamenazas*–, separada o conjuntamente, constituyen una de las mayores preocupaciones a nivel internacional y nacional, en el campo de la legislación penal. Esta creciente preocupación se manifiesta en el elevado número de convenios, acuerdos y reformas que en relación a los mismos pueden encontrarse. Sin embargo, lo que despierta un mayor interés radica precisamente en el uso de la informática como instrumento específico para la comisión de tipos delictivos y su creciente potencialidad de daño. De ahí que quizás, en primer lugar, trazaré a modo telegráfico un marco del estado de la cuestión a nivel mundial, para después pasar al ámbito europeo y terminar con el modelo español.

Grandes líneas de la situación a escala mundial

La diferente evolución económica y tecnológica se corresponde generalmente con similar grado de desarrollo normativo. De aquí la gran diferencia entre países en esta materia.

(19) WALL, *ob.* y *loc cit.*

(20) Por todos, ver ORTS BERENGUER, E., y ROIG TORRES, M., «*Delitos informáticos y delitos comunes cometidos a través de la informática*», Valencia, 2001.

En el área de África del Norte (Magreb), el bajo índice de utilización de internet, comporta una escasa preocupación estatal por el problema y consecuentemente un prácticamente inexistente marco normativo. Muy parecida es la situación en el África Subsahariana.

El lado opuesto lo encarna la zona de América del Norte, donde los gobiernos califican esta materia como atinente a la seguridad nacional y el desarrollo comercial de las nuevas tecnologías encuentra su nivel más alto (técnicas de biometría, tarjetas inteligentes, redes privadas virtuales, criptografía, redes inalámbricas WLAN, etc.).

En América Latina, en términos generales, la preocupación por la ciberseguridad sigue siendo en la actualidad secundaria. Comienzan paulatinamente a incorporarse los procedimientos internacionales de seguridad de la información, aunque existen todavía importantes vacíos jurídicos, como por ejemplo en relación al cifrado.

La ausencia de un marco legislativo sobre seguridad en las redes en la mayoría de países de Asia, permite de una parte el libre juego de empresas y consumidores, y de otra, una creciente intervención de los Gobiernos, que se proyecta sobre la gestión de los contenidos, la identificación, el filtrado y los sistemas de criptografía.

La característica más determinante de Oriente Medio es la explotación de las telecomunicaciones en régimen de monopolio por operadores nacionales. No se han desarrollado hasta el momento normativas importantes sobre seguridad de la información.

Del escenario europeo me ocupo a continuación con un mayor detenimiento.

Convenio del Consejo de Europa, sobre cibercriminalidad

Ha de hacerse una mención especial al Convenio del Consejo de Europa, sobre cibercriminalidad, firmado en Budapest el 23 de noviembre de 2001, el cual ha sido ratificado por España el pasado 3 de junio, y en vigor desde el 1 de octubre de 2010.

Tiene como propósito el lograr una mayor cooperación entre los Estados, así como el desarrollo de una legislación armonizada y apropiada para contener, en la mayor medida posible, este tipo de delincuencia. Se articula en cuatro capítulos, además del Preámbulo: el primero dedicado a definiciones; el segundo a disposiciones de derecho penal sustantivo

y procesal; el tercero a cooperación internacional; y el cuarto a las cláusulas finales (21).

En lo que respecta a los comportamientos, que necesariamente han de ser configurados como ilícitos penales en las correspondientes legislaciones internas, se estructuran en las siguientes categorías.

A) Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos informáticos (Tít. 1). En este grupo se deben describir como infracciones penales las siguientes conductas: a) acceso ilícito doloso y sin autorización a sistemas informáticos (art. 2); b) la interceptación dolosa e ilícita, sin autorización, a través de medios técnicos, de datos informáticos, en el destino, origen o en el interior de un sistema informático (art. 3); c) los atentados contra la integridad de los datos, consistente en dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos (art. 4); d) los atentados contra la integridad del sistema, esto es, la obstaculización grave, dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos (art. 5); e) el abuso de equipos e instrumentos técnicos, que comporta la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de dispositivos principalmente concebidos o adaptados para cometer las infracciones antes referidas; la de una palabra de paso (contraseña), de un código de acceso o de datos similares que permitan acceder a un sistema informático; y la posesión de alguno de los elementos antes descritos (art. 6)(22).

B) Infracciones informáticas (Tít. 2). Entre ellas, según este Convenio, deben sancionarse penalmente los siguientes comportamientos: a) las falsedades informáticas, que contienen la introducción, alteración, borrado o supresión dolosa y sin autorización, de datos informáticos, generando datos no auténticos (art. 7); b) estafa in-

(21) Por todos, ver, DE LA CUESTA ARZAMENDI y DE LA MATA BARRANCO (directores): «Derecho penal informático», Madrid 2010; GONZÁLEZ RUS: «Los ilícitos en la red (I): *hackers, crackers, cyberpunks, sniffers*, denegación de servicio y otros comportamientos semejantes», en «El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales», Granada 2006; FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, Oviedo 2007.

(22) GALÁN MUÑOZ: «Ataques contra sistemas informáticos», *Boletín Información Ministerio de Justicia*, 2006; GÓMEZ NAVAJAS: *La protección de datos personales*, Madrid 2005.

formática, que precisa la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de la introducción, alteración, borrado o supresión de datos informáticos, o de cualquier otra forma de atentado al funcionamiento de un sistema informático, siempre con la intención fraudulenta de obtener un beneficio económico (art. 8) (23).

C) Infracciones relativas al contenido. Sin embargo, dentro de este apartado únicamente se describen conductas relativas a pornografía infantil (art. 9).

D) Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines (art. 10) (24).

El Convenio también contiene disposiciones técnicas respecto a la sanción de la complicidad, la tentativa (art. 11), la responsabilidad de las personas jurídicas (art. 12) y las sanciones y medidas a imponer (art. 13).

En síntesis, desde la perspectiva penal sustantiva, se trata del primer instrumento normativo en el ámbito europeo, lo que de por si supone un paso decisivo hacia la armonización de las legislaciones en esta materia. Ahora bien, no debe confundirse armonización con unificación, pero en cualquier caso constituye el presupuesto necesario para la cooperación internacional y para avanzar hacia una mayor integración legal. En este sentido, como toda norma internacional, establece los mínimos comunes que los Estados miembros están obligados a incorporar a sus ordenamientos, pero desde luego no fija los máximos de intervención punitiva. En otro orden de consideraciones, aunque el texto se refiere a comportamientos cometidos en el ciberespacio, algunos de ellos no dejan de ser estructuras típicas tradicionales, que bien por el medio comisivo empleado (nuevas tecnologías) o bien por la mayor gravedad de su uso, se incluyen dentro de esta categoría.

En cuanto a las disposiciones de naturaleza procesal, en lo referente al ámbito de aplicación, se faculta a los Estados para que instauren procedimientos o procesos específicos para la investigación de los ilícitos penales antes descritos; o de cualquier otro delito cometido a través de un sistema informático, o para la recogida de pruebas electrónicas (art. 14). Igualmente advierte que los Estados velarán para que se respeten las garantías y derechos individuales proclamados en

(23) GALÁN MUÑOZ, A., «*El fraude y la estafa mediante sistemas informáticos*», Valencia, 2005.

(24) MIRÓ LINARES: «Internet y delitos contra la propiedad intelectual», Madrid 2005.

la normativa interna de cada Estado y especialmente en la normativa internacional (art. 15).

Relevante es la obligación de los Estados de disciplinar la conservación inmediata de datos (art. 16), así como la de conservación y divulgación inmediata de los datos de tráfico (art. 17). De igual modo deben adoptar medidas tendentes a la identificación o mandato de comunicación (art. 18), al registro y decomiso de datos informáticos almacenados (art. 19), a la recogida en tiempo real de datos informáticos (art. 20) y a la interceptación de datos relativos al contenido (art. 21).

De gran interés la regulación de la competencia, que insta a los Estados para que se atribuyan jurisdicción respecto a cualquier infracción penal contenida entre los arts. 2 a 11 del presente Convenio, cuando la misma se haya cometido en su territorio, a bordo de una nave que ondee pabellón del Estado; a bordo de una aeronave inmatriculada en ese Estado, o por uno de sus súbditos (art. 22). En este sentido, advertir que el Convenio mantiene el principio de la territorialidad como criterio de atribución de competencia, y no introduce reglas de ampliación o extensión de la jurisdicción.

En lo relativo a la cooperación internacional, junto a los principios generales (art. 23), se estipulan las reglas de extradición (art. 24), y un conjunto de medidas de colaboración y asistencia (arts. 25 a 35). Todo ello supone un significativo avance para la persecución e investigación de estos ilícitos.

Recordar asimismo el Protocolo Adicional sobre incriminación de actos de naturaleza racista y xenófoba, cometidos a través de sistemas informáticos, aprobado por el Consejo de Europa el 30 de enero de 2003. Con este Protocolo, anclado en la protección de los derechos fundamentales, se corrige una importante laguna del Convenio, persiguiéndose la armonización en este sensible ámbito.

Otros instrumentos normativos de la Unión Europea

También en el ámbito de la UE se han desarrollado numerosos instrumentos para la regulación de las nuevas tecnologías y su afectación a los derechos individuales, como por ejemplo ya iniciaron el Convenio 108/81 del Consejo, de 28 enero, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; o la Directiva 95/46CE del Parlamento Europeo y del Consejo de 24 de

octubre de 1995, relativa a la protección de los datos personales de las personas físicas y a la libre circulación de estos datos; luego seguidas de una abundante normativa.

Más recientemente, debe destacarse la Directiva 2000/31/CE del Parlamento y del Consejo Europeo, de 8 de junio, con la finalidad de armonizar los ordenamientos europeos en materia de servicios de la sociedad de la información. La misma se conoce como «comercio electrónico», y parte de la idea de crear un espacio europeo sin barreras en la comunicación e información. Sin embargo, ya advierte de la necesidad de intervención penal frente a determinadas conductas que pueden afectar a cuatro grandes áreas necesitadas de tutela: menores, dignidad humana, consumidores y salud pública.

En esta tendencia se inscribe la Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Aquí se fijan una serie de obligaciones de confidencialidad y regulación de la conservación de datos, prohibiendo la escucha, grabación, almacenamiento u otras clases de intervención o vigilancia de las comunicaciones. Sin embargo, debe subrayarse la introducción de excepciones a estas prohibiciones cuando se vea afectada la seguridad nacional (art. 15). La reciente Directiva 2006/24/CE, sobre conservación de tráfico de las comunicaciones electrónicas consagra esta orientación, tendente a garantizar la identificación del origen, destino, fecha, hora y duración de comunicaciones, el tipo de comunicación, el equipo utilizado y la localización del mismo, por razones de seguridad nacional.

Otro hito significativo en este camino de lucha contra la cibercriminalidad, lo representa la Directiva 2000/375/JAI, destinada a la adopción de medidas, fundamentalmente de actuación policial, para la persecución de conductas de pornografía infantil.

A destacar también la Decisión marco 2001/413/JAI del Consejo, de 28 de mayo, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo (DO L 149 de 2.6.2001); la más reciente Decisión Marco 2004/68/JAI del Consejo de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil (DO L 13/44 de 20.01.2004), en la que se hace referencia a la regulación de estos delitos cuando son cometidos a través de Internet. Y finalmente, la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero relativa a los ataques de los que son objeto los sistemas de información

(DO L 69 de 16.3.2005), por la que se establece la obligación de los Estados miembros de configurar como infracciones penales el acceso ilícito a un sistema de información, el perjuicio a la integridad de un sistema o la intromisión ilegal en los datos. Todas las cuales contienen indicaciones relativas a la realización de tales conductas a través de sistemas de comunicación.

Criminalidad organizada y terrorismo

La criminalidad organizada ha sido a su vez, objeto de una importante labor internacional. Así, debe hacerse referencia en primer lugar a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, adoptada por la Asamblea General de las Naciones Unidas el 15 de noviembre de 2000, mediante la Resolución A/RES/55/25, la cual tiene como objetivo, precisamente, lograr una mayor cooperación internacional en la lucha contra este tipo de delincuencia. O la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo (DO L 309 de 25.11.2005) (25).

La misma afirmación cabe hacer respecto del terrorismo, en relación al cual puede hablarse además de los respectivos Convenios firmados en el seno de la ONU, del Convenio del Consejo de Europa sobre prevención del terrorismo, firmado en Varsovia, el 16 de mayo de 2005, del cual también es parte nuestro país –aunque no ha sido ratificado–. Como es sabido, la estrategia que se ha venido estableciendo para combatir al terrorismo ha consistido en el incremento de la cooperación y del intercambio de la información, estableciéndose medidas concretas en relación a específicos aspectos relacionados con las mismas, tales como la facilitación de los procesos de entrega de los detenidos por estos delitos, mediante la Decisión Marco 2002/584/JAI del Consejo de 13 de junio de 2002 relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, transpuesta a nuestro ordenamiento mediante la Ley 3/2003 de 14 de marzo, sobre la orden europea de detención y entrega (BOE núm. 65, de 17 de marzo de 2003).

(25) VVAA: GONZÁLEZ CUSSAC, J. L. y FERNÁNDEZ HERNÁNDEZ, A., coord: *Financiación del terrorismo, blanqueo de capitales y secreto bancario. Un análisis crítico,* Valencia, 2009; FERRÉ OLIVÉ, J.C., y ANARTE BORRALLO, E., *Delincuencia organizada. Aspectos penales, procesales y criminológicos*, Universidad de Huelva, Huelva, 1999.

O la afectación de los recursos económicos de las organizaciones terroristas mediante la aprobación del Convenio Internacional para la represión de la financiación del terrorismo de 1999 de Naciones Unidas; la Resolución del Consejo de Seguridad de Naciones Unidas 1373, de 28 de septiembre de 2001; la Recomendación del Consejo de la Unión Europea, de 9 de diciembre de 1999, relativa a la Cooperación en la lucha contra la financiación de grupos terroristas; la Decisión marco del Consejo de 13 de junio de 2002, sobre la lucha contra el terrorismo o la Declaración de la Unión Europea sobre la lucha contra el terrorismo, de 25 de marzo de 2004 (26).

Como se aprecia, abundante es la normativa que a nivel internacional puede encontrarse sobre cada uno de los aspectos a los que se ha hecho referencia. Los ejemplos acabados de reseñar ponen de manifiesto sin embargo, dos tendencias que revisten, a nuestro modo de ver, una relevancia considerable. En primer lugar, que las actuaciones previstas versan sobre aspectos específicos que pueden ser individualizados en cada una de las categorías criminógenas referidas. En segundo lugar, que mediante el tratamiento individualizado de cada una de esos aspectos, se están comenzando a establecer instrumentos aplicables conjuntamente a las mismas. Sin duda, porque en la realidad cotidiana de las mismas, los vínculos de unión entre ellas son constantes e innegables.

Derecho penal español

Por lo que se refiere a España, el terrorismo, la criminalidad organizada y determinados delitos relacionados con las nuevas tecnologías encuentran respuesta en nuestro ordenamiento jurídico mediante su previsión, principalmente, en el Código Penal. En este sentido ya el Código Penal de 1995 supuso un avance de gran calado en estas materias, y la reforma del mismo de 2010, que entrará en vigor a partir del próximo 23 de diciembre de 2010, incorpora diversos instrumentos internacionales referidos a las nuevas tecnologías.

Igualmente hay que destacar el avanzado tratamiento que la literatura científica española ha venido realizando de estos fenómenos delictivos, conformando una consolidada y abundante doctrina al respecto. Lo mis-

(26) GONZÁLEZ CUSSAC, J. L. y FERNÁNDEZ HERNÁNDEZ, A.: «*Sobre el concepto jurídico-penal de terrorismo*», en «El Estado de Derecho frente a la amenaza del nuevo terrorismo», en «Teoría y Derecho. Revista de pensamiento jurídico «(Tirant), nº 3, junio 2008, págs. 34 a 58.

mo cabe decir de nuestra jurisprudencia, con un abundante cuerpo de resoluciones en la materia. A este amplio acerbo jurídico me remito y aquí únicamente me detendré en exponer esquemáticamente los principales ejes del sistema legal español (27).

Comenzaré por reseñar la importante modificación del Código Penal de 2010 en materia de «organizaciones y grupos criminales» (Cap. VI del Tít. XXII). En primer lugar, se contiene una novedosa regulación de los delitos cometidos en el seno de organizaciones o en grupos, en el que se distinguen ambos niveles de concierto de personas para cometer delitos. Aquí, además del castigo agravado por la comisión de concretas infracciones, se castiga como figura autónoma la pertenencia a las mismas (arts. 570 bis; ter; y quáter). Además de la sanción correspondiente por la comisión de los delitos comúnmente vinculados al crimen organizado, el modelo español contempla penas agravadas precisamente cuando éstos se realizan en el seno de las mismas. A tales efectos resulta igualmente relevante la definición que de la delincuencia organizada se contiene en el art. 282 bis de la LECrim.

A continuación, el Capítulo VII se refiere a las «organizaciones y grupos terroristas y a los delitos de terrorismo» (arts. 571 a 580), en el que se encuentra una detallada y completa –en relación a la normativa internacional y Derecho comparado– tipificación de estos ilícitos. Así, junto a la definición de organización y grupo terrorista, se sancionan, entre otras, las conductas de pertenencia y colaboración a las mismas (art. 571); la comisión de concretos delitos graves por personas que pertenecen, actúan a su servicio o colaboran (art. 572); el depósito y tenencia de armas, municiones y explosivos (art. 573); realización de infracciones menos graves por personas que pertenezcan, actúen a su servicio o colabores con organizaciones o grupos terroristas (art. 574); comisión de delitos contra el patrimonio para allegar fondos (art. 575); actos de colaboración, vigilancia e información (art. 576); actos de financiación (art. 576 bis); los que sin pertenecer colaborasen con las finalidades terroristas (art. 577); apología del terrorismo (art. 578); actos preparatorios (art. 579); y, reincidencia internacional (art. 580).

El escenario difiere sin embargo en lo que a las nuevas tecnologías se refiere. Al igual que ocurre por ejemplo en Italia o en Alemania, nuestro

(27) Con carácter general puede verse VIVES ANTÓN; ORTS BERENGUER; CARBONELL MATEU; GONZÁLEZ CUSSAC; MARTÍNEZ-BUJÁN PÉREZ. «Derecho Penal. Parte especial», 3ª ed. Valencia 2010.

legislador no ha optado por desarrollar un tratamiento conjunto y unitario de las conductas tipificadas penalmente, sino que por el contrario, dada la heterogeneidad de supuestos, se ha optado por ir ubicando en los distintos Títulos, Capítulos y Secciones que configuran el Código Penal, los ilícitos que pueden encontrarse relacionados con ellos. En efecto, también en materia de delitos vinculados a las nuevas tecnologías, el texto punitivo español mantiene el criterio sistematizador del bien jurídico tutelado (intimidad, patrimonio, etc.).

También en este ámbito deben subrayarse importantes modificaciones operadas por la reforma penal de 2010. En todo caso, expondré a continuación las principales figuras delictivas vinculadas con las nuevas tecnologías:

– concertación de encuentros con menores de trece años, a través de internet, teléfono o cualquier otra tecnología de la información o la comunicación, con la finalidad de atentar contra su indemnidad sexual (art. 183 bis);
– prostitución y corrupción de menores (art. 189);
– acceso ilícito a datos o programas informáticos (art. 197,3º);
– descubrimiento, revelación y cesión de secretos por personas encargadas o responsables de los soportes, ficheros informáticos, electrónicos o telemáticos (art. 197,5º);
– robo con fuerza: descubrimiento de claves para acceder a lugar cerrado y concepto de «llaves falsas» extendido a instrumentos tecnológicos de apertura y cierre (arts. 238 y 239);
– estafa informática: manipulación informática para lograr transmisión patrimonial no consentida; fabricación, introducción, posesión y facilitación de programas informáticos específicamente destinados a la comisión de estafas; utilización abusiva de tarjetas de crédito o débito, cheques de viaje o datos allí contenidos (art. 248,2º);
– defraudaciones de fluido eléctrico y análogos (art. 255);
– daños informáticos: borrado, alteración, supresión o hacer inaccesible datos, programas informáticos o documentos electrónicos; obstaculizar o interrumpir el funcionamiento de un sistema informático (art. 264); daños a medios o recursos de las Fuerzas Armadas (art. 265);
– propiedad intelectual (arts. 270 y 271);
– propiedad industrial (arts. 273 a 277);
– descubrimiento, revelación y difusión de secretos de empresa (arts. 278 y 279);

– la fabricación o tenencia de programas de ordenador específicamente destinados a cometer delitos de falsedades (art. 400);
– infidelidad en la custodia de documentos y violación de secretos por autoridad o funcionario público (arts. 413 y ss.);
– desórdenes públicos: obstaculizar o destruir líneas o instalaciones de telecomunicaciones (art. 560,1º);
– descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional (arts. 598 y ss.).

Aunque con ciertas imprecisiones técnicas y algún aspecto discutible, parece convenirse que nuestro ordenamiento penal contiene una adecuada regulación en la materia y un al nivel de incorporación de la normativa europea e internacional.

UN BALANCE DEL DEBATE JURÍDICO ACTUAL

Categorías Generales

La combinación de varios factores ya enunciados en el primer apartado, ha propiciado el nacimiento o el replanteamiento de una serie de complejas cuestiones jurídicas. A efectos meramente expositivos, éstas las podemos agrupar y enumerar como sigue:

A) En el ámbito del Derecho Constitucional, las nuevas tecnologías obligan a una profunda consideración de los siguientes aspectos: a) derecho fundamental a la intimidad (18.1 CE); b) derecho fundamental a la inviolabilidad del domicilio (18.2 CE); c) derecho fundamental al secreto de las comunicaciones (18.3 CE); d) derecho a la no intromisión en el entorno digital (18.4 CE); e) *Habeas data*; f) libertad de expresión e información (art. 20 CE).
Algún ejemplo puede servir para expresar esta preocupación. En principio, se suele aceptar que internet, como red de redes sobre la que no gobierna nadie, no conoce fronteras. Pero en algunos de los regímenes autoritarios más poderosos si se están tejiendo límites muy estrictos. Es el caso de China e Irán, que han invertido sustanciosas cantidades en TIC para controlar radicalmente la libertad de expresión en sus conexiones a la red, interceptando «webs» para capturar disidentes políticos, que luego son detenidos. En la actualidad ya no se conforman con cerrar páginas o censurar resultados en motores de búsqueda, sino que son capaces de espiar al internauta a través de sus proveedores de co-

nexión: leen sus correos electrónicos o *blogs* restringidos y controlan al detalle qué páginas visitan. El empleo de esta tecnología lesiona gravemente el derecho fundamental a la intimidad.

En efecto, pues internet funciona como una red de puertos conectados a sistemas autónomos, pequeñas redes que se unen en una gran red de redes no gobernada por nadie. Cada proveedor de una de esas redes se compromete a facilitar, en principio, que cada puerto, desde su dirección IP, comparta información –correos electrónicos, intercambio de archivos, visitas a páginas *web*– con otros puertos, en cualquiera de las demás redes autónomas. Pero cuando es un Estado, o cualquier corporación, quien controla esos puertos, puede interferir absolutamente en la navegación de sus usuarios: prohibiendo la comunicación entre dos o más puertos; desconectando a internautas; espiando o censurando los paquetes que transmiten la información en la red. Los conocidos conflictos de Yahoo (2004) y Google (2009) con el gobierno de China expresan suficientemente este grave problema. Pero idéntica pretensión han manifestado recientemente Arabia Saudí, Emiratos Árabes, Líbano, Argelia e India. Ahora solicitan el acceso al sofisticado sistema codificado de la telefonía móvil de Blackberry; este último país alegando que fue utilizado para preparar y ejecutar los recientes atentados de Bombay. Probablemente la siguiente empresa en ser requerida será Skype.

Pero esta capacidad técnica para controlar la información en la red, despertó la preocupación en gobiernos de Estados de Derecho, ante el posible abuso por parte de las grandes corporaciones. El ejemplo más evidente lo encontramos en los proveedores de internet de los Estados Unidos, que bajo la justificación de combatir lo que consideran *piratería*, emplean estas técnicas. Así sucedió en 2008 con *Comcast*, proveedora de banda ancha por cable, que según La Comisión Federal de Comunicaciones, estaba interfiriendo selectivamente sobre ciertas conexiones de programas P2P.

Lo mismo puede suceder cuando las agencias de seguridad apelan a la defensa de la seguridad nacional. Esta posibilidad obliga a una regulación legal precisa que impida prácticas arbitrarias, garantizando el derecho a la intimidad de los ciudadanos. Pues obvio es, que no solo los regímenes autoritarios están interesados en el control de las comunicaciones. La censura del blog de la embajadora del Líbano en Londres, el pasado verano, por elogiar al fallecido ayatolá Mohamed Hussein Fadlallah, considerado

mentor de Hizbulá y calificado de terrorista, es un buen ejemplo de esta tendencia. Ello obliga a la búsqueda de un equilibrio entre las libertades civiles y la seguridad nacional, que afecta por igual a Gobiernos y empresas tecnológicas.

En este contexto tampoco puede dejar de citarse la viva controversia por las revelaciones de documentos clasificados por el sitio web WikiLeaks, en torno a actuaciones de las fuerzas armadas norteamericanas durante los conflictos de Irak y Afganistán.

B) Por su parte, las nuevas tecnologías también obligan a que en el seno del Derecho Penal se proceda a una mayor precisión en la tipificación y proporcionalidad de la sanción de los siguientes comportamientos: a) delitos contra la intimidad: acceso ilícito; interceptación ilícita; descubrimiento de secretos e interceptación de comunicaciones; descubrimiento de secreto informático; b) crimen organizado y delincuencia profesional: fraudes informáticos; blanqueo de capitales; c) ciberterrorismo; d) atentados contra la integridad de datos e integridad del sistema (daños); e) fraudes informáticos: falsedad informática y estafa informática; f) responsabilidad de las personas jurídicas; g) pornografía infantil.

Así, no son pocos los problemas que en relación a la delincuencia informática pueden ponerse de manifiesto. Especialmente desde que el uso de Internet no sólo se ha generalizado, sino que se ha estandarizado. Las amenazas que la misma puede implicar para la intimidad o para el propio patrimonio, junto con el alto grado de evolución que tales técnicas experimentan, hacen que la actualización y análisis de las mismas deban ser constantes.

Dado que con las comunicaciones telemáticas las fronteras se tornan inexistentes y los espacios pierden su materialidad, a nivel jurídico pueden encontrarse multitud de problemas relativos a la determinación del lugar de comisión de los delitos, el momento en el que pueden considerarse cometidos, el esclarecimiento de la jurisdicción competente, así como la determinación de los sujetos a los que cabe atribuir responsabilidad por la comisión de los mismos.

A estos efectos, evidente resulta la controversia relativa a los *service-providers*. Pero los problemas que surgen en esta materia no lo son únicamente a efectos procesales, sino que también en materia de Derecho penal sustantivo pueden encontrarse aspectos problemáticos. Principalmente, la plasmación en un texto punitivo

de las conductas que a través de estos medios pueden llevarse a cabo, en particular sobre el derecho a la intimidad, dada la especial relación entre usuarios y servidores (28). Pero no sólo eso. Al igual que existen conductas que pueden ser cometidas mediante las nuevas tecnologías, respecto de las que nadie pone en duda su carácter delictivo, también puede aludirse a todo un conjunto de comportamientos que no sólo no se encuentran configurados como tales en la actualidad, sino que en determinadas ocasiones pueden ser reconocidos incluso como derechos, y de los que sin embargo, se está haciendo un uso del que pueden beneficiarse los grupos criminales organizados. Sin duda este es uno de los principales problemas con los que el legislador debe enfrentase. Los denominados usos pasivos que de internet y los ordenadores están realizando las organizaciones criminales para facilitar su organización y actuación constituyen sin duda, el objetivo sobre el que procede comenzar a trabajar inmediatamente.

Pero lo que ahora se pretende es centrar la atención en los novedosos procedimientos tecnológicos de los que hacen uso las organizaciones criminales en general y las terroristas en particular, a fin de poder desarrollar un balance de los instrumentos legislativos con los que contamos para afrontar esta nueva realidad. Es decir, que el uso ilícito de las nuevas tecnologías fuerza además a una tipificación altamente especializada y precisa, en constante transformación y evolución. Por citar un ejemplo de gran interés, el empleo de Internet para la propaganda y radicalización terrorista (29), o para la realización de operaciones de información de contrainsurgencia (30).

---

(28) KERR, I. & GILBERT, D.: «The Role of IPS in The Investigation of Cybercrime», en Tom Medina & Johannes J. Britz, *Information Ethics in the Electronic Age*, *Mendina, Johannes Brtiz, eds., McFarland Press, 2004*, pp. 163 a 172.

(29) LARRIBA HINOJAR: «Globalización, terrorismo y libertad de expresión: conminación penal de actividades terroristas en el entorno virtual», en «*Constitución, derechos fundamentales y sistema penal*» (Dir. Carbonell Mateu/González Cussac/Orts Berenguer), Valencia 2009; p. 1089 y ss.

(30) TAIPALE, K. A.: «Seeking Symmetry on the Information Front Confronting Global Jihad on the Internet», National Strategy Forum Review, Vol. 16, summer 2007; TAIPALE, K. A.: «Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance», *NYU Review of Law & Security, No. 7, Supl. Bull.on L. & Sec., Spring 2006;* TAIPALE, K. A: «Cyber-Deterrence», *Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global,* 2010.

C) En el campo del derecho procesal, han de destacarse las problemáticas relativas a: a) competencia y jurisdicción: aplicación extraterritorial de la ley penal; cooperación internacional; extradición y euroorden; b) medios de investigación y prueba: interceptación de comunicaciones; diligencia de entrada y registro y confiscación de discos duros; registro y decomiso de datos informáticos almacenados; recogida en tiempo real de datos informáticos; interceptación de datos relativos al contenido; interceptación de datos externos o de tráfico; c) responsabilidad del *service provider.*

La competencia jurisdiccional en los cibercrímenes es un asunto complicado y difícil, en particular cuando se refiere al terrorismo (31). En este sentido, acciones en Internet que son legales en el país donde se inician pueden ser ilegales en otros países, incluso aunque el acto no sea particularmente fijado como objetivo en ese único país (32).

Los conflictos sobre la competencia jurisdiccional pueden ser tanto negativos –ningún Estado reclama la competencia–, como positivos –varios Estados reclaman dicha competencia–. Pero por encima de todo lo que no está claro es qué constituye la competencia jurisdiccional: ¿Es el lugar donde se lleva a cabo la acción?, ¿El país de residencia de quien comete la acción?, ¿El lugar donde se producen los efectos de la acción?, ¿O el país cuya nacionalidad tiene el propietario del ordenador que ha sido objeto de ataque?, ¿O todos ellos a la vez? Como es sencillo observar, tras estos interrogantes se esconden diversas cuestiones jurídicas: el *forum delicti commissi*; el principio territorial; la atribución de competencia a las diferentes jurisdicciones nacionales, etc.

En todo caso, de lo que no cabe duda es que los países no se ponen completamente de acuerdo sobre esta cuestión y tienen visiones muy diferentes, produciéndose así una divergencia global. Es más, los diversos estatutos sobre el cibercrimen que han sido aprobados en las últimas décadas en numerosos países, muestran una amplia variedad de cláusulas diversas sobre la competencia jurisdiccional (33).

---

(31) TRACHTMAN, J. P.: «Global Cyberterrorism, Jurisdiction, and International Organization», Tufts University, The Fletcher School, July 20, 2004.

(32) BRENNER, S. W. & KOOPS, B-J.: «Approaches to Cybercrime Jurisdiction», Journal of High Technology Law Vol IV No 1, 2004, pp. 3 a 46.

(33) REIDENBERG, J. R.: «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, Vol 153:1951, 2005, pp. 1951 a 1974.

Por otra parte, ya se ha aludido a la interceptación y censura en anteriores apartados, ahora solo quiero hacer mención al incremento del uso de tecnologías para bloquear sitios con contenidos ofensivos y su posterior tráfico. El caso paradigmático es la pornografía infantil. En este sentido sobresale su empleo por unidades policiales de países tan variados como los EEUU, México, Holanda o España. Y en general, debe llamarse la atención para garantizar que la investigación policial de actividades delictivas se desarrolla conforme a reglas constitucionales de confidencialidad y proporcionalidad.

De otra parte, me parece crucial hacer referencia a la problemática de la investigación criminal ultraterritorial o transfronteriza (34). Un conocido caso puede servir de muestra.

En otoño de 2000, el FBI se enteró de que unos hackers habían penetrado en las redes informáticas de bancos, grandes grupos empresariales, proveedores de servicios de Internet y otras firmas norteamericanas. Ante la sospecha de que los ataques provenían de Rusia, el FBI intentó, sin éxito, asegurarse la asistencia de Rusia para la monitorización y reparación de la actividad criminal. Tras este fallido intento, los Estados Unidos decidieron actuar unilateralmente. Después de obtener una orden de registro en los USA, empleó un programa rastreador («sniffer») de registro de pulsación de tecla, para conocer los nombres de usuario y contraseñas de los hackers. Esta información fue empleada, a su vez, para bajar información incriminatoria de los ordenadores de los hackers en Rusia.

Las acciones descritas del FBI son conocidas como *«remote cross-border searchers and seizures»*, expresión que se puede traducir como búsquedas e incautaciones remotas transfronterizas (o fronterizas). Actualmente, las búsquedas e incautaciones de esta clase son una importante herramienta en la lucha contra el cibercrimen.

Los robos transfronterizos, los sabotajes de un sistema, los gusanos, y los ataques de denegación de servicio, causan, hoy por hoy, un enorme daño a los sistemas informáticos en los Estados Unidos y en otros países. Y para poder castigar esos crímenes,

(34) GOLDSMITH, J. L.: «The Internet and the Legitimacy of the Remote Cross Border Searches», *Chicago Public Law and Legal Theory Research Paper No. 16*, The Law School, University of Chicago, 2001, pp. 1 a 15.

es crucial identificar la procedencia del ordenador del que parte la actividad criminal e incautar (o al menos inmovilizar) información relevante para el crimen antes de que la grabación sea eliminada o borrada. No hay que olvidar aquí, que la demanda de información acerca de la actividad de ordenadores que están en el extranjero –o dicho con otras palabras, fuera de las fronteras del propio país– se incrementó de manera significativa tras los ataques terroristas del 11S de 2001.

Ciertamente, una manera de obtener información sobre ordenadores que están en el extranjero es a través de la cooperación entre los organismos oficiales encargados de aplicar la ley en el país fijado como objetivo –en el ejemplo planteado al principio, los Estados Unidos– y los del país de origen –en el ejemplo planteado al principio, Rusia–. El problema es que, a menudo, esta cooperación es harto difícil. Así pues, algunas veces, el gobierno del país de origen de los ataques carece de la autoridad legal para incautar e inmovilizar información de un ordenador más allá de sus fronteras. Algunas otras, de lo que carece es de capacidad tecnológica. También porque su maquinaria legal es demasiado lenta para hacer frente a un tipo de crimen en el que las pruebas pueden ser rápidamente destruidas o convertidas en anónimas. O, simplemente, el país de origen no quiere cooperar.

Por las razones descritas, y por muchas otras, las autoridades del país fijado como objetivo se pueden encontrar con capacidad para resolver ellos mismos el problema. Sentados en sus ordenadores, pueden trazar los orígenes del cibercrimen, y explorar, recabar y almacenar información relevante localizada en ordenadores que están en el extranjero.

En la doctrina, muchos autores entienden que esas búsquedas e incautaciones remotas transfronterizas, violan la soberanía territorial del país donde los datos son localizados. Este punto de vista parece encontrar apoyo en las prohibiciones de aplicación ultraterritorial de la ley recogidas en instrumentos jurídicos de Derecho Internacional. Frente a estas opiniones, se formulan otras en las que se argumenta que las búsquedas e incautaciones remotas transfronterizas son acordes con los principios internacionales que rigen la aplicación de la ley. No afirman, no obstante, que no deban existir límites en esas búsquedas e incautaciones, sino que esos límites no deben deducirse de normas relativas a la territorialidad. En su lugar, los límites tendrán que emerger de un complica-

do proceso de examen y regulación jurídica transnacional, desde el momento en que las naciones han de ajustarse ellas mismas a los cambios crecientes de las nuevas tecnologías. Esto es, apelan a la necesidad de arrojar algo de luz en la relación entre el cambio tecnológico y la evolución de nuestros conceptos jurídicos (35).

Por último, decir que, al argumentar que las citadas búsquedas e incautaciones remotas transfronterizas pueden ser legales, desde el punto de vista jurisdiccional, estos autores no niegan que el ejercicio de estas pueda ser problemático. Es más, entienden que, aunque esas búsquedas e incautaciones estén justificadas en el terreno jurisdiccional, pueden ser injustificables desde la perspectiva de los derechos fundamentales individuales de privacidad (intimidad) y de libertad de expresión.

D) Otra cuestión de enorme complejidad es, después de analizar las medidas legislativas existentes en nuestro ordenamiento jurídico, con especial incidencia en las penales, en relación a los delitos informáticos y los delitos comunes cometidos a través de la informática cometidos en el seno de organizaciones criminales y especialmente terroristas, la interpretación y aplicación que vienen realizando nuestros Juzgados y Tribunales de justicia.

E) Por último, tras haber estudiado la normativa internacional relativa a estas materias, examinar el grado de integración de tales normativas en nuestro sistema legislativo, así como la necesidad de la misma, lo que obligará a fijarse en las dificultades y necesidades de adaptación que ello requiera.

Problemas Específicos

Después de exponer las categorías generales del Derecho afectadas por los usos y abusos de las nuevas tecnologías, dedicaré un último apartado a resaltar las cuestiones más específicas de esta creciente problemática.

A) En primer lugar, como ya se vio al examinar las respuestas legales, la situación varía considerablemente entre países y regiones, con diferente grado de implantación de las nuevas tecnologías y también con diferente grado de desarrollo de sus legislaciones. Estrechamente vinculado a este diagnóstico, se encuentra el dato de que más de 45 países han firmado el Convenio de Ciberde-

(35) GOLDSMITH, *ob.* y *loc.cit.*

lincuencia, tanto en el espacio del Consejo de Europa, como en el de Naciones Unidas. Sin embargo, aún dentro de este selecto grupo de naciones, se observa una distinta escala de operatividad del mismo, debida a múltiples circunstancias, entre ellas la efectiva incorporación a los ordenamientos nacionales de las disposiciones internacionales (36).

B) Podría decirse, en términos generales, que aunque el modelo contenido en el Convenio funciona muy aceptablemente, en particular en el espacio europeo occidental y norteamericano, algunos Estados permanecen excesivamente absortos en sus prioridades y problemas internos. Esta actitud supone un desconocimiento de las ventajas globales de la cooperación y armonización internacional.

C) La tendencia marcada por el Convenio, así como su funcionamiento en general, merece una valoración altamente positiva. Especialmente porque contribuyó a la concienciación internacional sobre la magnitud y evolución de este problema, logrando consensos políticos mínimos acerca de las conductas a prohibir y de los mecanismos de persecución y colaboración jurisdiccional. Pero también porque significó un gran avance técnico-jurídico, por ejemplo, al propiciar definiciones legales estándar, posibilitar la extradición y fortalecer la cooperación policial y judicial entre Estados.

D) Sin embargo, el crecimiento de la cibercriminalidad no se debe imputar únicamente a las insuficiencias legales, ya sean al definir los ilícitos, al establecer los procedimientos procesales o regular la cooperación de las agencias de seguridad, sino que también obedece, y en gran medida, a la simple negligencia de las personas, incluso en áreas de la alta seguridad sumamente profesionalizada. Por ejemplo, un soldado sueco ha sido declarado culpable por negligencia al haber perdido una memoria USB en un ordenador de la Universidad de Estocolmo, con detalles sobre bombas sin explosionar en Afganistán. O que el ejército norteamericano esté tomando medidas contra el uso de memorias USB tras la infección de redes de defensa con el gusano SillyFDC. O los numerosos supuestos de espionaje, fraude o robo de datos por la apertura del correo electrónico sin tomar las medidas de seguridad mínimas (37).

---

(36) HANSSEN, H-S.: «The Future of International Law: Cybercrime», *Regional Meeting of ASIL*, Golden Gate University School of Law, 17 Annual Fulbright Symposium on The Future of International Law, San Francisco, 7 April, 2007.

(37) MENN, J.: «Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet», Perseus Books, 2010.

E) Ahora bien, los logros anteriormente reseñados no pueden valorarse como absolutos ni como permanentes. Por ello, para finalizar, señalaré algunos de los problemas específicos pendientes de resolver en el plano jurídico.

1. A pesar de los avances del Convenio en esta materia, sigue siendo un reto de máxima prioridad alcanzar consensos sobre las definiciones legales, esto es, sobre la tipificación precisa y exacta de los comportamientos declarados como delitos. Sólo si la normativa internacional facilita el acuerdo acerca de lo que es delito, esto es, armoniza el Derecho penal de los diferentes Estados al describir las figuras delictivas, podrá realmente articularse una efectiva cooperación internacional. En efecto, pues si compartimos tipos delictivos similares o idénticos, entonces podremos desarrollar adecuadamente procedimientos de extradición, intercambio de pruebas y de otra clase de informaciones. De ahí la esencial transcendencia de este enorme desafío y el objetivo de corregir las cláusulas de escape detectadas en el Convenio.
2. El transcurso del tiempo y la constante innovación tecnológica han causado que el Convenio, en ciertas materias, haya quedado parcialmente obsoleto y por consiguiente tengamos la necesidad de actualizarlo. En este sentido, y a título de ejemplo, pueden citarse conductas graves no contenidas en el Convenio, como el *phishing*, la suplantación de identidad, o los delitos cometidos en mundos virtuales (v. gr. el *atraco* en la red social Habbo Hotel). A la necesidad de actualizar la legislación contribuye el constante progreso de las nuevas tecnologías, pues hoy, por ejemplo, con un simple iPod se puede copiar toda la información de un ordenador que carezca de una protección adecuada. También se discute la necesidad de sancionar penalmente a las empresas que no comunican a los usuarios y a las autoridades «brechas de seguridad» en sus servidores.
3. Por fin, aunque el Convenio ha supuesto un extraordinario adelanto –aunque como hemos visto insuficiente– para la armonización de la legislación penal, adolece sin embargo de un desarrollo normativo avanzado en materia de cooperación policial. Es decir, se precisa un esfuerzo legislativo tendente a facilitar las necesidades operativas, habida cuenta de la todavía inercia policial a la actuación dentro de sus fronteras respectivas. Así, mientras la ciberdelincuencia está organizada, comparte

información y actúa en cualquier parte del mundo, se hace imprescindible que las fuerzas de seguridad posean herramientas similares: organismos internacionales *ad hoc;* intercambio de información en tiempo real e instrumentos de cooperación transfronterizos. Los aislados éxitos en este campo, como por ejemplo la reciente operación secreta del FBI en colaboración con otros cuerpos policiales, contra el foro denominado «Dark Market», avalan esta necesidad y posiblemente muestran la escasa eficacia hoy existente.

En definitiva, como expone el informe del Parlamento Europeo de 2 de marzo de 2010**,** es sumamente necesaria una normativa unificada internacional, para detener la gran cantidad de abusos, robo de identidad y demás delitos virtuales que realizan casi a diario los atacantes informáticos. La propuesta, básicamente, se basa en la creación de un conjunto de normas internacionales que definan taxativamente los actos delictivos en internet, y posibiliten la reducción de las altas cotas actuales de impunidad en la que se escudan los atacantes informáticos por la falta de normativas unificadas, por parte de la comunidad internacional, que impiden que sean castigados o capturados si se encuentran en un país remoto, al lugar al que atacaron.

La finalidad es minimizar los ataques, tanto personales como corporativos y gubernamentales, que traen consigo fraudes, robos de identidad y hasta espionaje. Aún está reciente el ataque a Google proveniente de Asia, zona que alberga una gran cantidad de atacantes que se escudan en una legislación local obsoleta y permisiva, que les facilita la comisión y posterior impunidad de delitos cometidos fuera de sus fronteras.

Por tanto, unas legislaciones armonizadas a nivel mundial permitirían a los Estados, a las corporaciones y a los particulares afectados, salvar el obstáculo de las fronteras y poder investigar, capturar y enjuiciar a los atacantes en cualquier lugar del mundo donde se encuentren –incluso si utilizan servidores Proxy–, ya que sería más sencillo ubicarlos.

En este citado Informe, se aconseja que los miembros de La Unión Europea, que poseen los mejores sistemas en línea, deben realizar un acercamiento directo en tema de ciberseguridad con países no pertenecientes a la UE, como Estados Unidos, China y Rusia, para tratar de unificar sus legislaciones e incrementar la cooperación, con el objetivo de disminuir los delitos virtuales.

De igual forma, la Unión Europea debería desarrollar una estrategia similar a la contenida en la Iniciativa Nacional de Ciberseguridad norteamericana. Como se ha conocido recientemente, en la misma se fija el objetivo de establecer estrategias efectivas para blindar las transacciones bancarias y financieras, las redes de transporte por superficie, subterráneas, aéreas y marítimas, y la protección digital de las infraestructuras de comunicaciones civiles y militares, de energía, transporte, seguridad militar, e informática, de toda la nación. Con ello se trata de evitar que los ciberatacantes provoquen apagones masivos, detengan la actividad comercial y financiera, cometan fraudes a particulares y entidades financieras, o alteren el funcionamiento de las redes de seguridad informáticas civiles y militares.

Idéntica orientación ha tomado la doctrina militar rusa en materia de seguridad en la información, como se ha publicado parcialmente en febrero de 2010 en un documento no clasificado.

CONCLUSIONES

La primera conclusión se centra en la mutación expansiva de la categoría jurídica de seguridad nacional, que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta uno más amplio y multidimensional como es el de seguridad nacional. Ahora bien, este nuevo concepto todavía en formación, no ha acabado de perfilarse con la suficiente concreción jurídica, discurriendo en numerosas ocasiones entre su entendimiento como idea simbólica-emotiva, o como equivalente a interés general identificado con el interés del Estado y contrapuesto al interés individual. De aquí que el usual manejo del canon de ponderación de intereses para resolver los conflictos entre seguridad nacional y derechos fundamentales, casi siempre se resuelve a favor del primero.

En segundo lugar, nos hallamos ante un nuevo escenario estratégico, criminológico y político-criminal, en el que se aprecia no sólo un salto cuantitativo sino también cualitativo. Y en este sentido se habla de una ruptura: los escenarios de ataques son muy variados, con diferentes niveles de riesgo y de muy diversa escala de impacto potencial, lo que complica extraordinariamente su prevención y respuesta estatal. Ahora el *nuevo terrorismo y la nueva criminalidad transnacional*, se muestran con una mayor agresividad y representan un auténtico desafío para los

Estados. Pero su control igualmente hace peligrar los valores del Estado de Derecho, especialmente la de los derechos fundamentales.

En tercer lugar, el desarrollo del ciberespacio ha facilitado enormemente el desarrollo de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales. Hoy en día se ha encaminado el control de muchos procesos mundiales a través del ciberespacio. Por lo que no hay duda de que actualmente el ciberespacio constituye un bien valioso. Y de que la seguridad del ciberespacio ha crecido en importancia.

En cuarto lugar, ha de tenerse presente que a la profesionalización, internacionalización y globalización de la criminalidad, se suma la consolidación del uso de las tecnologías de la información y la comunicación (TIC), obtenemos los ejes esenciales que configuran la realidad sobre la que gira este trabajo. En este sentido, en sí mismas las TIC constituyen instrumentos de alto valor patrimonial, político y estratégico; pero tampoco deben minusvalorarse las facilidades que el uso de las nuevas tecnologías ofrece para la ejecución de ilícitos, lo que a su vez conlleva la generalización y aumento del recurso a estas tecnologías como instrumento comisivo.

En quinto término, podría decirse que *cibercrimen* y *ciberamenazas* no son categorías equivalentes, pues existen ciberdelitos que no constituyen amenazas a la seguridad nacional, ni todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética. Ahora bien, en los supuestos mencionados –terrorismo y criminalidad organizada–, determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional.

Y en sexto y último lugar, afirmar que la combinación de varios de los factores enunciados, ha propiciado el nacimiento o el replanteamiento de una serie de complejas cuestiones jurídicas, tanto relativas a los derechos fundamentales, como a cuestiones penales sustantivas y procesales. En este sentido, la tendencia marcada por el Convenio sobre Cibercriminalidad, así como su funcionamiento en general, merece una valoración altamente positiva. Sin embargo, el transcurso del tiempo y la constante innovación tecnológica han causado que el Convenio, en ciertas materias, haya quedado parcialmente obsoleto y por consiguiente tengamos la necesidad de actualizarlo. En este sentido, y a título de ejemplo, pueden citarse conductas graves no contenidas en el Convenio, como el *phishing*, la suplantación de identidad, o los delitos cometidos

en mundos virtuales. Igualmente se hace preciso reforzar y avanzar en materias como la competencia ultraterritorial y también en cooperación policial internacional.

BIBLIOGRAFÍA

ALBANESE, J.S., DAS, D.K., y VERMA, A., (editores), *Organized crime.* World perspectives, New Jersey, 2003;

ARQUILLA, J., y RONDFELDT, D., *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo político*, Madrid, 2002;

ARTEAGA: «La estrategia europea de seguridad: cinco años después», ARI nº 15/2009, Real Instituto Elcano, 22/01/2009.

BANDINI, T., *La criminalità organizzata*, Torino, 1993.

BALLESTEROS MARTÍN, M. A.: «*El papel de las fuerzas armadas en la lucha contra el terrorismo internacional*», en Real Instituto Elcano de Estudios Internacionales y Estratégicos, 18/08/2006.

BERDAL, M., y SERRANO, M., (editores), *Transnacional organized crime and internacional security: business as usual?*, Colorado, 2002.

BOIX REIG (dir.) y JAREÑO LEAL (coord.): «La protección jurídica de la intimidad», Madrid 2010;

BRENNER, S. W. & KOOPS, B-J.: «Approaches to Cybercrime Jurisdiction», Journal of High Technology Law Vol IV No 1, 2004, pp. 3 a 46.

CARRASCO ANDRINO: «El delito de acceso ilícito a los sistemas informáticos», en «Comentarios a la reforma penal de 2010», (Dir. F. Álvarez García y J. L. González Cussac), Valencia (Tirant), 2010;

CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010;

Convenio Internacional sobre el cibercrimen, 23 de noviembre de 2001 (Council of Europe CETS No 185).

[disponible en**:** http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm]

Coordinator for Counterterrorism (NCTb), *Jihadist and the internet*, Delta-Hage, La Haya, 2007, pp. 17 y ss.

[disponible en www.fas.org/irp/world/netherlands/jihadis.pdf]

CUADRADO RUIZ: «Interceptaciones telefónicas y nuevas tecnologías», en *Cuadernos Jurídicos* 1992;

DE LA CUESTA ARZAMENDI y DE LA MATA BARRANCO (directores): «Derecho penal informático», Madrid 2010;

DÍAZ SANTOS, M.R., y FABIÁN CAPARRÓS, E. A., «*El sistema penal frente a los retos de la nueva sociedad*», Madrid, 2003.

Doctrina militar rusa y seguridad en la información: [disponible en**:** www.belt.es/expertos/HOME2_experto.asp?id=4999]

Cybersecurity FBI. [disponible en**:** www.fbi.gov/cyberinvest/cyberhome.htm]

FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, Oviedo 2007.

FERNÁNDEZ RODRÍGUEZ y SANSÓ-RUBERT PASCUAL (editores): «Internet: un nuevo horizonte para la seguridad y la defensa» (Seminario de Estudios de Seguridad y Defensa de la USC-CESEDEN). Universidad de Santiago de Compostela 2010;

FERRÉ OLIVÉ, J.C., y ANARTE BORRALLO, E., *Delincuencia organizada. Aspectos penales, procesales y criminológicos*, Universidad de Huelva, Huelva, 1999.

FOJÓN CHAMORRO y SANZ VILLALBA: «Ciberseguridad en España: una propuesta para su gestión», ARI 101/2010, Real Instituto Elcano 18/06/2010;

FREUND, W., *Die Strafbarkeit von Internetdelikten*, Wien, 1998.

GALÁN MUÑOZ, A., «*El fraude y la estafa mediante sistemas informáticos*», Valencia, 2005;

GALÁN MUÑOZ: «Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática», en Revista de derecho y proceso penal, 15, 2006;

GALÁN MUÑOZ: «Ataques contra sistemas informáticos», *Boletín Información Ministerio de Justicia*, 2006;

GOLDSMITH, J. L.: «The Internet and the Legitimacy of the Remote Cross Border Searches», *Chicago Public Law and Legal Theory Research Paper No. 16*, The Law School, University of Chicago, 2001, pp. 1 a 15.

GÓMEZ NAVAJAS: *La protección de datos personales*, Madrid 2005;

GÓMEZ TOMILLO, M., *Responsabilidad penal y civil por delitos cometidos a través de internet. Especial consideración del caso de los Proveedores de contenidos, servicios, acceso y enlaces*, 2ªedic., Pamplona 2006.

GONZÁLEZ CUSSAC, J. L.: «*Nuevas amenazas a la seguridad nacional: el desafío del nuevo terrorismo»*, en «Retos de la política criminal actual», Revista Galega de Seguridade Pública (REGASP)«, nº 9, Xunta de Galicia, 2007, pp. 233 a 252;

GONZÁLEZ CUSSAC, J. L. y FERNÁNDEZ HERNÁNDEZS, A.: «*Sobre el concepto jurídico-penal de terrorismo»*, en «El Estado de Derecho frente a la amenaza del nuevo terrorismo», en «Teoría y Derecho. Revista de pensamiento jurídico «(Tirant), nº 3, junio 2008, pp. 34 a 58;

GONZÁLEZ CUSSAC, J. L: «*Intromisión en la intimidad y servicios de inteligencia»*, en «La protección de la intimidad», Cursos de Formación de Fiscales, Madrid (CEJ), 2010**;**

GONZÁLEZ CUSSAC/LARRIBA HINOJAR: «Un nuevo enfoque legal de la inteligencia competitiva», en »Inteligencia y Seguridad: Revista de análisis y prospectiva», nº 8, 2010, pp. 39 y ss.;

GONZÁLEZ RUS**: «**Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», Rev. De la facultad de Derecho de la Universidad Complutense, 12; 1986;

GONZÁLEZ RUS**: «**Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264,2 CP)», en La ciencia del derecho penal ante el nuevo siglo: homenaje al Prof. Cerezo Mir, Madrid 2002;

GONZÁLEZ RUS: «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en «El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales», Granada 2006;

GUISASOLA LERMA: «*Tutela penal del secreto de las comunicaciones. Estudio particular del supuesto de interceptación ilegal de telecomunicaciones por autoridad o funcionario público»,* en «Constitución, derechos fundamentales y sistema penal» (Dir. Carbonell Mateu/González Cussac/Orts Berenguer), Valencia (Tirant) 2009;

GÜNTER, R., *Computer criminalität*, bhv, 1998.

GUTIÉRREZ FRANCÉS, M.L., «*Fraude informático y estafa*», Madrid, 1991;

HANSSEN, H-S.: «The Future of International Law: Cybercrime», *Regional Meeting of ASIL*, Golden Gate University School of Law, 17 Annual Fulbright Symposium on The Future of International Law, San Francisco, 7 April, 2007.

HOFFMAN, B., «The Use of the Internet by Islamic Extremists», [disponible en www.rand.org]

Informe del Parlamento Europeo de 2 de marzo de 2010, [disponible en www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2010-0026+0+DOC+XML+V0//ES]

JAREÑO LEAL y DOVAL PAIS: «Revelación de datos personales, intimidad e informática», en *La Ley*, 4844, 1999;

JIMÉNEZ CAMPOS: «*La garantía constitucional del secreto de las comunicaciones*», en Comentarios a la legislación Penal, tomo VII, Madrid (Edersa) 1986;

JOFER, *Strafverfolgung im Internet. (Phänomenologie und Bekämpfung kriminellen Verhaltens in internacionalen Computernetzen)*, Frankfurt a. M., 1999;

KERR, I. & GILBERT, D.: «The Role of IPS in The Investigation of Cybercrime», en Tom Medina & Johannes J. Britz, *Information Ethics in the Electronic Age*, *Mendina, Johannes Brtiz, eds., McFarland Press, 2004*, pp. 163 a 172;

LARRIBA HINOJAR: «Globalización, terrorismo y libertad de expresión: conminación penal de actividades terroristas en el entorno virtual», en «Constitución, derechos fundamentales y sistema penal» (Dir. Carbonell Mateu/González Cussac/Orts Berenguer), Valencia (Tirant) 2009; p. 1089 y ss.:

LEWIS, J.: «Security Cyberspace in the 44th Presidency», Report 2008.

LÓPEZ ORTEGA: «La intimidad como bien jurídico protegido», en *Estudios sobre el Código Penal de 1995* (Parte Especial), *CGPJ*, Madrid 1996;

LÓPEZ ORTEGA: «Intimidad informática y Derecho Penal (la protección penal de la intimidad frente a las nuevas tecnologías de la informa-

ción y comunicación)», en *Derecho a la intimidad y nuevas tecnologías*, CDJ 2004;

MADRID CONESA: «*Derecho a la intimidad informática y Estado de Derecho*», Valencia, 1984;

MARCHENA GÓMEZ: «Intimidad e informática: la protección jurisdiccional del *habeas data*», en *BIMJ*, 1996;

MARCHENA GÓMEZ: «El sabotaje informático: entre los delitos de daños y desórdenes públicos», Cuadernos de Derecho Judicial, 10, 2001;

MATA Y MARTÍN: «*Delincuencia informática y Derecho Penal*», Madrid 1996;

MATA Y MARTÍN: «La protección penal de datos como tutela de la intimidad de las personas: intimidad y nuevas tecnologías», *RP* 2006;

MATELLANES RODRÍGUEZ: «El intrusismo informático como delito autónomo», *RGDP* 2004;

MENN, J.: «Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet», Perseus Books, 2010;

MIR PUIG (editor): «*Delincuencia informática*», Barcelona, 1992;

MIRÓ LINARES: «Internet y delitos contra la propiedad intelectual», Madrid 2005;

MORALES PRATS: «*La tutela penal de la intimidad: privacy e informática*», Madrid, 1984;

MORALES PRATS: «Servicios de información y espionaje del Estado y secreto de comunicaciones telefónicas», en *Actualidad Aranzadi*, 253, 1996;

MORÓN LERMA, E., «*Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red*», 2ª ed., Pamplona 2002.

ORTS BERENGUER: «Revelación y uso indebido de secretos e informaciones», en *CDJ (Delitos de los funcionarios públicos),* Madrid 1994;

ORTS BERENGUER, E., y ROIG TORRES, M., «*Delitos informáticos y delitos comunes cometidos a través de la informática*», Valencia, 2001.

PANSIERA, F. J., y JEZ, E., «*La criminalité sur l´internet*», Puf, 2000;

PICCOTI, L., (Coord.), «*Il diritto penale dell´informatica nell´epoca di internet*», Padova, 2004.

QUINTERO OLIVARES: «Internet y propiedad intelectual», en Cuadernos de derecho judicial, 10, 2001;

REBOLLO BARGAS: «*La revelación de secretos e informaciones por funcionario público*», Barcelona 1996;

REIDENBERG, J. R.: «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, Vol 153:1951, 2005, pp. 1951 a 1974.

RODRÍGUEZ MOURULLO/LASCURAIN SÁNCHEZ/ALONSO GALLO: «Derecho penal e internet», en «Régimen jurídico de internet», Madrid 2001;

ROGAN, H., *Jihadism online – A study of how al-Qaeda and radical islamist groups use the Internet for terrorist purposes,* FFI/RAPPORT-2006/00915, [disponible en http://rapporter.ffi.no/rapporter/2006/00915.pdf];

ROMEO CASABONA, C. M., «*Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*», Madrid, 1987.

ROMEO CASABONA: «La protección penal del «software» en el Derecho español», *AP* 35, sept-oct. 1988;

ROMEO CASABONA: «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», *P.J.,* 31, 1993;

ROMEO CASABONA: «*Los delitos de descubrimiento y revelación de secretos*», Valencia 2005;

ROMEO CASABONA (coord.): «*El Cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas políticocriminales*», Granada 2006;

RUEDA MARTÍN: «Protección penal de la intimidad personal e informática: los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal», Barcelona 2004;

RUIZ MARCO, F., «*Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*», Madrid, 2001.

SÁNCHEZ GARCÍA DE PAZ: «La criminalidad organizada. Aspectos penales, procesales, administrativos y policiales», Madrid, 2005.

SERRANO PIEDECASAS: «Consideraciones en torno a la protección penal del «Knowhow», *ADPCP*, III, 1990;

SIEBER, U., (editor), «*Information technology crime*», Köln, 1994;

SHULMAN, C.: «Medidas del Consejo de Europa para luchar contra la cibercriminalidad», en ENAC, nº 2, agosto 2009, p. 31.

TAIPALE, K. A.: «Seeking Symmetry on the Information Front Confronting Global Jihad on the Internet», National Strategy Forum Review, Vol. 16, summer 2007.

TAIPALE, K. A.: «Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd», *Yale Journal of Law and Technology,* Vol. 7, No. 123, December 2004, pp. 123 a 201.

TAIPALE, K. A.: «Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance», *NYU Review of Law & Security, No. 7, Supl. Bull.on L. & Sec., Spring 2006;*

TAIPALE, K. A: «Cyber-Deterrence», *Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global,* 2010;

TAIPALE, K. A «Internet and Computer Crime: System Architecture as Crime Control», *Center for Advanced Studies Working Paper No. 03-2003*, 2003.

TRACHTMAN, J. P.: «Global Cyberterrorism, Jurisdiction, and International Organization», Tufts University, The Fletcher School, July 20, 2004.

VVAA: «Cybercrime & Security», New York 2005;

VVAA: González Cussac J. L. y Fernández Hernández A. coord. «Financiación del terrorismo, blanqueo de capitales y secreto bancario. Un análisis crítico«, Valencia, 2009;

VIVES ANTÓN; ORTS BERENGUER; CARBONELL MATEU; GONZÁLEZ CUSSAC; MARTÍNEZ-BUJÁN PÉREZ. «Derecho Penal. Parte especial», 3ª ed. Valencia 2010.

WALL, D. S.: «The Internet as a Conduit for Criminal Activity», Information Technology and the Criminal Justice System, Pattavina, A., ed. Sage Publications, Inc., 2005, pp. 77-98.

YAR: «Cybercrime and society», London 2006;

ZÚÑIGA RORÍGUEZ, L., / MÉNDEZ RODRÍGUEZ, C., / DIEGO DÍAS-SANTOS, M.R., (Coords.), «*Derecho Penal, sociedad y nuevas tecnologías*», Madrid, 2001.

CAPÍTULO TERCERO

EL CIBERESPACIO Y EL CRIMEN ORGANIZADO

EL CIBERESPACIO Y EL CRIMEN ORGANIZADO

JUAN SALOM CLOTET

RESUMEN

El increíble auge de las nuevas tecnologías ha supuesto un cambio en las relaciones e interacciones de la sociedad actual, donde usuarios, legisladores y gobiernos no acaban de vislumbrar la forma de ordenar la pacífica y libre existencia.

Por el contrario, el delincuente sí se ha amoldado rápidamente a ese nuevo escenario, aprovechando las ventajas de las deficiencias legislativas y del nuevo espacio jurídico. Su adaptación ha sido tal que se ha procurado un espacio de impunidad, que ha supuesto un efecto llamada para la delincuencia. Han desembarcado, de la mano de los expertos informáticos o hackers, con toda su fuerza, abriéndose paso las formas más avanzadas de la delincuencia, las bandas organizadas.

Palabras clave: Cibercrimen, ciberespacio, ciberpolicía, delito informático, incultura digital, paraíso informático, hacker, hacking, cracker, script kiddie, lammers, pirata informático, troyanos, caballo de troya, rootkit, código dañino, phishing, phisher, carding, skimming, scrow, pharming, vishing, smishing, CaaS, mulas, scam 419.

CYBERSPACE AND ORGANIZED CRIME

ABSTRACT

The incredible rise of new technologies has brought about changes in the relationships and interactions of today´s society, where users, le-

gislators and governments are not able to envision how to manage the peaceful and free existence.

On the other hand, offenders have quickly adapted themselves to this new situation, taking advantage of the weaknesses of the new legislation and legal framework. Their adaptation has been such that it has raised a space of impunity, which has been a knock-on effect for the crime. Organized gangs, the most evolved form of crime, have landed with all their force, and with the help of computer experts and hackers have pushed through the Internet.

Key words: Cybercrimen, cyberspace, ciberpolice, cibercrime, digital illiteracy, data haven, hacker, hacking, cracker, script kiddie, lammers, trojan, trojan horse, rootkit, malware, phishing, phisher, carding, skimming, scrow, pharming, vishing, smishing, CaaS, mules, scam 419.

INTRODUCCIÓN

El enorme desarrollo de las Nuevas Tecnologías, la informática y las telecomunicaciones, y especialmente el efecto sinérgico entre ambas, está suponiendo un cambio trascendental en la sociedad. Trabajo, economía, administración y ocio son algunos de los aspectos que están variando a pasos agigantados, dirigiéndonos hacia esa sociedad cada vez más global, en la que la esfera de influencia supera nuestro entorno mediato, y lo que ocurre en nuestras antípodas ya forma parte de nuestras circunstancias. En este nuevo modelo social, al que hemos bautizado como Sociedad de la Información, juega un papel determinante Internet como vehículo de transmisión e intercambio de todo tipo de información (1), produciéndose una sinécdoque entre la parte y el todo, Internet por Sociedad de la Información.

Internet, la red de redes, es factor determinante de la globalización cultural y, en especial, de los mercados, diseñando nuevos escenarios socioeconómicos. Sin ir más lejos, el comercio electrónico (*e-commerce*), abre un escenario de potenciales mercados internacionales, inima-

(1) Ver introducción de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

ginables para los actuales modelos de pequeñas empresas, que traerán consigo el desarrollo de servicios complementarios de transporte y precisarán de un esfuerzo imaginativo por parte de la administración para el control de la actividad fiscal.

La implantación de esta sociedad, que parece no conocer otro límite que la imaginación humana, puede incluso hacer tambalear los propios fundamentos del Estado y de la concepción actual del sistema democrático, dando paso quizá a una democracia electrónica (2) con la ya probada experiencia del voto electrónico, en la que cabría una participación que superara la simple elección de representantes para llegar a la toma de decisiones de forma cotidiana y directa por parte del ciudadano.

Estas situaciones reflejadas no son más que simples conjeturas de lo que esta Sociedad de la Información puede traer consigo, además del ya indiscutido incremento de la calidad de vida, apoyado en el desarrollo tecnológico.

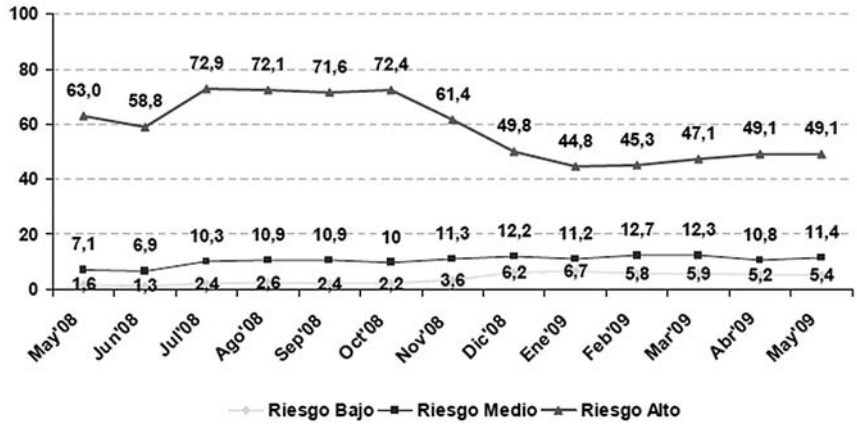
Por otro lado, Internet está vivo, está en un proceso de crecimiento imparable, tanto en servicios como en usuarios, afectando cada vez más a nuestra forma de vida. En la red proyectamos nuestro trabajo, es nuestro escenario de ocio, de comunicación, de negocio, en ella nos movemos, compramos, buscamos información y depositamos nuestra intimidad y privacidad, nuestra vida laboral y económica. Es un espacio común, al que denominamos «ciberespacio», que sirve a fines legítimos y positivos, pero que también ha traído nuevas situaciones sobre las que resulta precisa la intervención del Derecho. La protección de la información, de nuestra privacidad, regular las relaciones comerciales, o los derechos de propiedad intelectual no pueden quedar al arbitrio de los usuarios. Resulta preciso adecuar las normas al nuevo escenario, para evitar crear espacios de impunidad, que pueden ser aprovechados por unos pocos para hacer prevalecer sus intereses.

Ese mundo virtual basado en la tecnología digital, se ha convertido en un reto intelectual para unos y una barrera para otros. La complejidad técnica de los sistemas informáticos y del diseño de las redes, y los protocolos de comunicaciones que se utilizan, generan indudablemente diferencias de conocimiento entre los usuarios de la Red, que sin duda

(2) En este sentido ver informe del GOL (Goverment On Line) del G8, de 6 de diciembre de 2001, en el que se realiza un estudio de la adaptación de los Estados a una futura pero posible democracia electrónica.

son aprovechados por unos pocos para hacer prevalecer sus intereses. En este sentido cabe destacar los resultados de los estudios que realiza INTECO (3) sobre la seguridad de la información y la e-confianza de los hogares y de las PYMES españolas, en los que de forma reiterada, se obtienen valores de riesgo de los equipos informáticos que rondan el 50%.

Gráfico 15: Evolución del nivel de riesgo de los equipos (%)



Fuente: INTECO

Esa dificultad para comprender y conocer el mundo digital, de la que no es ajeno el legislador, también afecta al proceso legislativo sobre las nuevas tecnologías, amén de que la dinámica de éstas, sometidas a un vertiginoso y contante avance, sobrepasa la dinámica legislativa. El resultado es una inadecuación o vacío legal en torno a los aspectos de la Red, que afectan a todos los órdenes del Derecho, incluido el penal.

A ello hay que añadir la complejidad del escenario global, donde los tradicionales límites geográficos quedan desdibujados por la realidad del tráfico internacional de información y la interacción entre sujetos sometidos a distintas jurisdicciones con marcos legislativos distintos, lo que sin duda da lugar a espacios de impunidad o *paraísos informáticos,* en los

(3) INTECO (Instituto Nacional sobre Tecnologías de la Comunicación) Realiza periódicamente estudios sobre los niveles de confianza de los usuarios domésticos y PYMES, que se pueden descargar en http://www.inteco.es/Seguridad/Observatorio.

que el control normativo, por intereses superiores o por nivel de desarrollo de la sociedad, no existe o es muy permisivo.

Por último, Internet se revela como un mundo virtual donde no existen los mismos patrones sociales del mundo real, un mundo al que nos asomamos ocultos tras la pantalla, creyendo ser anónimos y asumiendo nuevos roles. Donde la protección que ofrece la facilidad de crear identidades ficticias, supone un acicate o desinhibidor de nuestros temores frente a las barreras sociales, impulsándonos a veces a superar la legalidad establecida.

A la incultura digital, al escaso rechazo social de las conductas desviadas en la red, al vacío legal y al anonimato de la red, que ya de por sí son estímulos para el delincuente, se suma el rechazo social a cualquier medida restrictiva orientada a la seguridad. La idea romántica de una red como máximo exponente de la libertad de expresión está muy arraigada. Cualquier medida de control es interpretada como una potencial amenaza a la intimidad de las personas como derecho fundamental, lo que lleva a una defensa cada vez más férrea de ésta, incluso frente al intervencionismo de los Estados para la protección de sus ciudadanos, interpretado como un intento de crear una «*sociedad orweliana*» (4).

Este conjunto de circunstancias nos ha llevado a una sociedad de la información, a un ciberespacio, inseguro, donde las alarmas van creciendo día a día y la inseguridad es cada vez mayor.

La expresión más representativa de esa inseguridad, de ese lado oscuro de la red, es lo que socialmente entendemos como el cibercrimen.

EL DELITO INFORMÁTICO

El Ciberdelito, cibercrimen o delito informático es un concepto que manejamos socialmente para referirnos a un conjunto de conductas que vulneran los derechos de terceros y se producen en un escenario o medio tecnológico, provocando un rechazo social y sobre las que media el derecho penal.

Pero la idea es muy amplia. Las nuevas tecnologías están presentes en muchas facetas de nuestra vida. Qué duda cabe que el enraiza-

(4) George Orwell, en su novela «1984», imaginó una sociedad controlada por el Estado, el «Gran Hermano» que todo lo ve. La novela fue publicada en 1949.

miento de los medios tecnológicos es tan grande que están en todas partes. Por ello, casi no podemos imaginar la realización de cualquier delito sin que éstos aparezcan. El desvío de dinero a paraísos fiscales a través de transacciones electrónicas para evadir impuestos o blanquear dinero, la falsificación de moneda a través de medios tecnológicos, la apología de diversos tipos penales, la coordinación entre terroristas o bandas organizadas, las amenazas, la extorsión, etc. Prácticamente todo cabe. Y por ello, la idea de ciberdelito es cada vez más amplia o global.

Sin embargo, jurídicamente, el debate es más amplio y no hay consenso al respecto. Existen incluso los que niegan la existencia de estos delitos alegando que son delitos tradicionales que tienen encaje en los tipos penales actuales. Otros, por el contrario, defienden la necesidad de definir nuevos tipos.

El proyecto legislativo de mayor trascendencia, quizá el esfuerzo más serio y más ambicioso, el más consensuado a la hora de acotar el delito informático, ha sido el del Consejo de Europa. Su Consejo de Ministros nombró, en 1997, un Comité de Expertos del Ciberespacio, integrado por policías, juristas e informáticos, y al que se invitó a su participación a países no europeos pero con un peso especial en la sociedad de la información global (EE.UU, Canadá, Japón y Australia), para debatir los problemas que generaba una incipiente delincuencia en Internet. Tras cerca de cuatro años y veinticinco borradores con distintas revisiones, logró poner de acuerdo a la comunidad internacional con su Convenio sobre Ciberdelincuencia, aprobado y abierto a la firma por el Plenario del Consejo de Ministros en Budapest, el 23 de noviembre de 2001.

Este Convenio pretende armonizar la legislación de los diversos países que lo ratifiquen, no sólo en materia de derecho penal sustantivo, sino también de derecho procesal para hacer frente a ese tipo de delincuencia.

El Convenio define los delitos informáticos agrupándolos en cuatro grupos:

a) Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.
   Engloba las conductas de acceso ilícito, interceptación ilícita, interferencia de datos, interferencia de sistemas y el abuso de dispositivos.

b) Delitos por su contenido.
   Comprende las conductas que se engloban en los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la Red.
c) Delitos relacionados con la informática.
   Se definen dos tipos penales, la falsificación informática y el fraude informático.
d) Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines.
   En este grupo el Convenio hace una remisión normativa a los tratados y convenios internacionales sobre propiedad Intelectual.

En un Protocolo adicional al Convenio, de enero de 2003, se incluyeron las conductas de apología del racismo y la xenofobia a través de Internet, como delitos de contenido.

El Convenio y su Protocolo adicional, se hicieron eco de las realidades sociales de algunos delitos, especialmente de los delitos de contenido, dándoles el estatus de delito informático. Conductas que hasta entonces existían en el mundo real, pasan a ser conductas prácticamente exclusivas del mundo virtual, es decir, delitos informáticos, puesto que ya no existe en otro medio que no sea el tecnológico. Incluso ha sido el medio tecnológico lo que ha fomentado el delito, pasando de ser una conducta esporádica en el mundo real, a un delito muy repetido en el mundo virtual.

Las mismas circunstancias de la pornografía infantil, se reproducen en otras conductas que en el momento de discusión del Convenio, no tenían cabida o no se llevaban a cabo en la red. Tal es el caso del acoso a menores a través de la red, conducta conocido en el argot de internet como *grooming*, las injurias y calumnias, las amenazas, el robo de identidad, el intrusismo laboral, conductas que la red está fagocitando. Por ello, podemos decir, sin temor a equivocarnos, que hay una pluralidad de conductas que, día tras día, van adquiriendo mayor incidencia social y que entonces, cuando se aprobó el Convenio, tenían nula o escasa incidencia, y por ello, la catalogación de delitos informáticos que hace el Convenio empieza a necesitar una revisión.

Es éste quizá, el único pero que se puede achacar al Convenio, el no haber previsto el dinamismo y crecimiento de la red. Sin embargo, supone un gran acierto el buscar la uniformidad de las normas penales y procesales de los países firmantes, para facilitar la persecución de un delito global, que no entiende de fronteras terrestres.

El Convenio, hasta la fecha, sólo ha sido firmado por 46 países y ratificado por 30 estados firmantes (5). España lo ratificó el pasado 3 de junio de 2010, y acaba de entrar en vigor el día 1 de octubre.

La importancia del Convenio no está tanto en el número de países que lo han firmado y ratificado sino en que se ha constituido en el referente internacional a la hora de hablar de la delincuencia informática, y de aproximarnos a una legislación global. Gran número de países, sobre todo latinoamericanos, que ha redactado leyes especiales para la delincuencia informática, como es el caso de Venezuela, Chile o Argentina, han tenido una clara inspiración en el Convenio.

DEL *HACKER* ROMÁNTICO AL PIRATA INFORMÁTICO

De los cuatro grupos de delitos que el Convenio de Ciberdelincuencia acota como informáticos, quizá el más informático de todos sea el conjunto de delitos contra integridad, confidencialidad y disponibilidad de datos y sistemas informáticos.

Tenemos la tendencia a definir Internet como la gran red de redes, otorgándole así, indirectamente, mayor valor a la red en sí que a la información que se almacena en ella, al mallado de cables que componen la red que a los datos que por ellos circulan. Son pues la información que circula por la red y la funcionalidad de ésta, su poder de tratamiento de información y de comunicación, el objeto de la protección penal. Que esa información se almacene y fluya en la red con garantías de integridad, confidencialidad y disponibilidad.

El funcionamiento de la red se basa en unos protocolos que permiten el envío de información, independientemente del tipo de información que sea y del sistema que la remite. Estos protocolos fueron ideados hace ya muchos años para un proyecto militar, Arpanet, en el que por su uso y naturaleza, no se contemplaba que pudieran ser interceptados. De igual forma, la información se almacena en sistemas gestionados por programas y sistemas operativos, que como toda obra humana, está sujeta a errores desde el punto de vista de la seguridad. Vemos pues que el medio es vulnerable y ello llevó a muchos usuarios, apasionados por

(5) Se puede ver la lista actualizada de los países firmantes y los que lo han ratificado en http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=29/06/2010&CL=ENG.

la tecnología, a buscar y detectar cualquier vulnerabilidad de las redes y sistemas. Sus pretensiones no eran dañinas, su afán de descubrir los fallos del sistema a veces les llevaba a superar barreras de confidencialidad, pero el marco legislativo, con su indefinición, les protegía. Eran los primeros *hackers*.

Aunque el termino *hacker* tiene sus orígenes en la vulneración de las redes telefónicas para efectuar llamadas gratuitas, accediendo a centrales o interceptando llamadas, con la extensión de la red para uso de la comunidad universitaria y científica, rápidamente se transmutó el significado, y socialmente se identificó al *hacker* con el experto informático que era capaz de detectar los fallos de programación y entrar en los sistemas informáticos vulnerando las medidas de seguridad. Eran los inicios de la socialización de la informática, donde ésta todavía era muy «árida» y poco usable, muy distinta a la informática de hoy en día. Para algunos se convirtió incluso en un estilo de vida, en un reto intelectual y personal. La red era su pasión y su vida. Eran los románticos de la red.

Socialmente no se les reprobaba. Más al contrario, se les consideraba mentes privilegiadas que causaban admiración. Se estaba creando el mito social del *hacker*, apoyándose en novelas (6), películas (7) y con estereotipos de comportamiento. Se estaba alimentando la cultura del «*hacking*», que lejos de verse como una conducta negativa y perjudicial para los derechos colectivos de los usuarios de internet, sigue hoy manteniendo esa connotación romántica y positiva.

Qué duda cabe que no todos aquellos *hackers* tenían una visión tan romántica de la red, ni todos respetaban por igual la confidencialidad ajena, pero en líneas generales, sí se podía hablar de *hackers* «no lesivos». Incluso entre ellos distinguían los que tenían pretensiones filantrópicas, de mejorar la red, y aquellos otros que les movía la ambición y los intereses delictivos, a los que llamaron crackers.

Con el crecimiento de la red y el triunfo de jóvenes *hackers* emprendedores que fundaron las principales empresas del sector, se consolidó el mito y la meta para el *hacker*, lograr alcanzar notoriedad con sus acciones en la red, para aspirar a destacados puestos profesionales, rodeados de todo tipo de prebendas económicas y sociales. El *hacker* que es contratado por una multinacional con sueldos astronómicos.

---

(6) STOLL Clifford, *The Cuckoo's Egg*, EE.UU, Doubleday, 1989, 326.
(7) Película Juegos de Guerra, EE.UU. año 1983.

Esta idea romántica del *hackers*, guardián o «Robin Hood» de la red, ha permanecido hasta nuestros días y, aún hoy, en la juventud, atraída por el escenario de la red y enmarcado en la rebeldía juvenil, se autoidentifican muchos como *hackers*.

Pero con la socialización de la red y su enorme crecimiento, las circunstancias han cambiado mucho. Los sistemas son cada vez más seguros pues la demanda social así lo exige y las empresas de desarrollo de software dedican más recursos a ello. Por el contrario, los conocimientos técnicos para detectar las vulnerabilidades han de ser muy altos y por ello, al alcance de muy pocos. El afán de comunicación y de divulgación de conocimientos que impera en la red, arrastra a todos, incluidos los *hackers*, que darán a conocer los fallos o errores de programación que descubran, quizá por ese afán de notoriedad que rodea a la personalidad del *hacker*. Otros, incapaces de detectarlos, los harán suyos, los utilizarán e incluso los adaptarán mediante programas automáticos, para que sean utilizables por terceros que, ni siquiera serán capaces de entender la vulnerabilidad o fallo de seguridad que están aprovechando. Así nacen los *script kiddies* o *lammers*, usuarios con conocimientos un poco superiores a la media, que se autodenominan *hackers* y dispuestos a vulnerar la legalidad para buscar protagonismo.

Dado el gran número de usuarios que se identifican con esta cultura del hacking, y que practican sin reparos acciones con menosprecio de los derechos de terceros, el concepto de *hacker* ha mutado semánticamente, pasando a identificar al *hacker* como el usuario de la red, que haciendo uso de conocimiento, técnicas y herramientas informáticas, actúa contra sistemas informáticos de terceros, aprovechando las vulnerabilidades y errores de configuración de los sistemas, vulnerando la legalidad.

Tal es la carga peyorativa del *hacker* que, aquellos que poseen los conocimientos técnicos adecuados, utilizando las mismas técnicas de los *hackers*, para prevenir la acción de éstos, prestan servicios de auditoría y seguridad de sistemas informáticos para detectar vulnerabilidades, debiendo calificar sus actuaciones, siempre legales, de hacking «ético» o «blanco».

Pero pese a esa transformación del *hacker*, parte de la sociedad todavía ve con buenos ojos al *hacker*, un joven travieso e inquieto, no identificándolo con el delito, para el que busca otros conceptos como «pirata informático».

El objetivo del *hacker* es encontrar fallos de seguridad en el software del equipo. En su sistema operativo o en las aplicaciones que tiene instaladas. Estos fallos de seguridad se conocen como *bugs* o agujeros de seguridad. Desde su descubrimiento hasta que se hace público entre los técnicos de seguridad y logran encontrar la corrección o *parche de seguridad*, es explotado por los delincuentes que desarrollan pequeños programas (*exploits*) que aprovechan esa vulnerabilidad permitiendo entrar en los sistemas y adquirir *privilegios de administrador*, es decir, acceder al sistema para gestionarlo y/o controlar la información. Normalmente, una vez dentro, el atacante se asegura poder entrar en el sistema cuantas veces quiera, dejando una vía de entrada oculta, a la que llaman *puertas traseras*.

Las primeras acciones de los *hackers*, buscando notoriedad, fueron la creación de los temidos virus o gusanos, programas maliciosos que se introducían en el ordenador y que causaban un daño más o menos leve. La diferencia entre los virus y los gusanos estaba en la capacidad de autorreplicación, es decir, en la capacidad de que un ordenador infectara a otros. La vía primera de distribución de esos virus era a través del intercambio de disquetes o CD.

Posteriormente los virus se empezaron a ocultar en otro programa o documento que al ejecutarse por el usuario, infectaba el sistema. Eran los *troyanos*, en alusión al Caballo de Troya que ocultaba en su interior soldados griegos para asaltar la inexpugnable ciudad de Troya. Para infectarse, la víctima debía aceptar el caballo, el atractivo regalo aparentemente inocuo, el programa gratuito que buscamos, la presentación con atractivas imágenes, el vídeo de moda, etc. El *vector de infección* más utilizado para hacernos llegar el atractivo regalo, que contiene oculto el programa malicioso, fue el correo electrónico. Hoy, los vectores de infección son muy diversos: las redes P2P que enmascaran los troyanos en videos musicales o películas; las descargas de software gratuito; los servidores web con contenidos dinámicos, que al visitarlos el usuario se descarga, sin saberlo, el programa malicioso, etc...

La solución contra los virus eran los antivirus, y frente a ellos, los *hackers* desarrollaban cada vez más virus y más complejos, algunos prácticamente indetectables, como los *rootkits*. Así, podemos afirmar que se ha entrado en una dinámica o espiral de acción reacción entre los *hackers* y las empresas de desarrollo de software y de seguridad de la información.

¿HACKING BY DOLLAR?

La Red evoluciona y día a día se hace más «usable», más intuitiva y fácil de manejar, pasando del modo comando, al alcance de unos pocos y en el que había que conocer complejas instrucciones alejadas del lenguaje humano, a sistemas mediante ventanas, muy intuitivos y fáciles de usar hasta para el usuario menos avezado. Esta evolución también se proyecta en el volumen de información que en ella se deposita. La red se ha convertido en un repositorio de datos personales, información que pertenece al ámbito de la privacidad de las personas. Nuestra intimidad circula por la red, nuestras relaciones sentimentales, orientaciones sexuales, conflictos personales con terceros, son habitualmente compartidos con amigos, parejas, compañeros, o simplemente almacenados en nuestros equipos informáticos. Pero no sólo se almacena o comparte información personal, también se comparte información empresarial y económica. Las estrategias de empresa, los planes de negocio, los secretos de empresa, los datos económicos, etc. Y esa información, tiene un valor, un valor económico.

Los *hackers* se dan cuenta de que el mito del contrato millonario en la empresa *punto com* ya no existe. Que frente al experto informático la empresa prefiere al titulado académico. Que sus actuaciones con afán de notoriedad, no le reportan beneficio. Que la capacidad de entrar en los sistemas ajenos, por sí sola no tienen valor. Que el valor está en la información que almacenan los sistemas. El objetivo final cambia, ya no es descubrir la vulnerabilidad de las redes o sistemas. Ese es un objetivo táctico. El objetivo estratégico es acceder a los sistemas para obtener la información.

La primera información objeto de su interés, es la que más relación directa guarda con el valor económico, la información financiera. Sus principales acciones se dirigen a obtener datos económicos. Información de tarjetas de crédito, cuentas bancarias, etc. Información que puedan convertir fácilmente en dinero o bienes. Para ello, se centrarán en el comercio electrónico, con las compras, utilizando tarjetas de crédito de terceros, conducta conocida como *carding*.

A partir del año 2002, con el incipiente servicio de banca electrónica, empiezan a buscar rentabilidad a sus acciones mediante la usurpación de las identidades online de banca electrónica para transferencias de dinero no consentidas. Sus técnicas de hacking se orientan al apode-

ramiento de las claves de acceso a banca electrónica, mediante la conjugación del engaño y la suplantación de portales de la banca. Nace el *phishing*.

Pero no todos los *hackers* buscan la rentabilidad económica de sus acciones. Siguen existiendo los *hackers* movidos por las banalidades y veleidades humanas, los conflictos personales. El robo de información a parejas por rencores anclados a la rotura de la relación; de información empresarial, para dañar la imagen, fama y honor de directivos intransigentes contra los que existe un enfrentamiento; o de la privacidad de terceros por buscar diversión o satisfacer las inclinaciones *voyeristas*.

Incluso, algunos persisten en su idea de ganar notoriedad en la red, realizando ataques a sistemas con resultados visibles para el resto de usuarios, que puedan firmar o autoimputarse. Estamos refiriéndonos a los ataques de *defacement* o modificaciones de páginas web, y a los ataques de denegación de servicio contra sistemas informáticos (8).

LA DELINCUENCIA ORGANIZADA

Pero las posibilidades de ganar dinero en la red, vulnerando la legalidad, no pasan desapercibidas para las mafias de la delincuencia organizada, que, advirtiendo que el escenario es nuevo y con deficiencias legislativas que juegan a su favor, decide irrumpir en este terreno. Éstas, aportan su experiencia y estructura organizativa para el crimen, pero necesitan de los conocimientos de expertos *hackers*. Así nace el maridaje entre la delincuencia organizada y el cibercrimen.

Los primeros escenarios de la delincuencia organizada se focalizan en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios. Por ello conviene conocer los distintos modus operandi de ambos fraudes, para entender el papel de la delincuencia organizada y su evolución, especialmente del segundo, del que derivan otras formas de delincuencia organizada, consecuencia de la especialización de determinadas actividades o etapas del delito, que se ofrecen como servicio al resto de organizaciones de-

(8) Una denegación de servicio o ataques DoS (Denial of Service), consiste en atacar la disponibilidad de los sistemas de información, evitando que puedan prestar el servicio para el que han sido concebidos. Es uno de los ataques más temidos por los administradores de sistemas, por su relativa facilidad de comisión y el peligro que supone para la imagen continuidad del negocio de las empresas afectadas.

lictivas. Tal es el caso de la llamada industria del malware y del comercio de información personal.

Por último, no hay que obviar otro tipo de delincuencia organizada, menos estructurada y técnica, pero también vinculada a la red, concretamente a los timos en la red.

Fraude en comercio electrónico

El comercio electrónico o la adquisición y venta de productos a través de la red, se realiza sin la mediación del comercial, lo que permite reducir costes. Su dinámica es muy sencilla, ofrecer productos a través de comercios electrónicos, abonarlos mediante el clásico sistema de tarjetas de crédito, utilizando sistemas de envío de dinero o mediante pago electrónico seguro (PayPal, MoneyBookers,…), y remitirlo por empresas de transporte.

Como podemos ver, el sistema es sencillo a la vez que frágil. La confianza que ofrece el vendedor se basa en la apariencia y el nombre de un comercio, y de unos productos que únicamente conocemos por lo que se ve en la web. Y como quiera que el comercio electrónico se está orientando hacia la venta entre particulares, la confianza queda muy mermada por desconocer al vendedor.

La fortaleza del sistema de pago reside en la robustez de las tarjetas de crédito o débito, sistema que ya de por si es frágil y que tiene un alto índice de fraude, pero que, en Internet, se acrecienta por la imposibilidad de acreditar la tenencia de la tarjeta y la identidad del titular de la misma. Una vez que se dispone de la numeración de una tarjeta de crédito/débito y su fecha de caducidad, se puede utilizar contra cualquier comercio electrónico utilizando una filiación falsa y un punto de entrega del producto «comprometido», bajo control del defraudador. Está técnica de pago con tarjetas fraudulentas se conoce como *carding*. El terminal de venta virtual del comercio electrónico establece comunicación con su entidad financiera y la única verificación que establecen para validar la compra es la validez de la tarjeta. Hoy en día, algunos comercios y entidades financieras, están exigiendo el Código de Seguridad de la Tarjeta (Card Security Code - CSC) o también llamado CVV (Card Verification Value - CVV o CV2), un nuevo valor numérico presente en el soporte físico de la tarjeta y que, teóricamente, acredita que el usuario de la misma la tiene físicamente en su poder.

Por último, el sistema de entrega del objeto de la compra es vulnerable toda vez que no existe un sistema de acreditación del titular destinatario del producto. Normalmente las empresas de mensajería y transporte, ante la ausencia de respuesta en un domicilio, dejan una notificación para acudir a la central de la empresa a recoger el porte, donde con la simple notificación ya es garantía para recibirlo. Si se dispone de un domicilio desocupado y el control del buzón, un defraudador ya tiene domicilio para direccionar la entrega.

Con este escenario, cabe imaginar que el fraude ha de existir. Si a ello añadimos el ingenio del defraudador para inducir a engaño a las víctimas, el resultado está garantizado.

Por último mencionar que el fenómeno del comercio electrónico ha evolucionado de los portales de venta hacia los portales de subastas o clasificados, donde el vendedor no es un comercial, sino particulares que compran y venden. El fraude, por la exigencia de previo pago, prácticamente solo cabe del vendedor hacia el comprador, es decir, simular una venta para cobrar y no entregar nada a cambio.

Veamos las formas más habituales del fraude en el comercio electrónico, en las que la delincuencia organizada ha focalizado su actuación.

El carding

Inicialmente, el fraude en el comercio electrónico se centró en duplicar portales de venta que inducían a engaño a las víctimas que abonaban dinero por productos que no recibían. La vida útil de las falsas web era muy escasa. Lo justo para engañar a unas pocas víctimas que denunciaban el fraude. La incidencia del fraude fue escasa e imputable a delincuentes esporádicos que actuaban de forma independiente.

Posteriormente, se pasó al *carding*, la compra de productos abonándolos con tarjetas de crédito falsas. Los defraudadores posteriormente revendían los objetos del fraude, a precios muy bajos, para obtener beneficios. La gran mayoría de estos fraudes se dirigieron contra comercios de productos informáticos, de telefonía móvil, con gran salida en el mercado, y billetes de transportes (tren, avión, barco). Esta dinámica de fraude exigía una estructura capaz de obtener tarjetas para las compras, infraestructura para la recepción de los productos y canales de venta posteriores de objetos procedentes del fraude, es decir, una mínima estructura organizativa, grupos organizados para delinquir.

En España estas organizaciones estaban y están formadas mayoritariamente por grupos de inmigrantes subsaharianos, y los canales de recepción y venta se centran sobre los propios miembros de la etnia, que les dan salida a través de la venta ambulante. Aunque mayoritariamente toda la operativa del fraude se realiza desde España, ocasionalmente se ha detectado que la fase de compra vía internet se realiza desde los países subsaharianos, si bien la entrega del producto se hace en España.

Conscientes de la vulnerabilidad que representa la entrega del producto objeto del fraude, los defraudadores utilizan lugares de entrega en los que se logre desvincular al receptor, del fraude, como por ejemplo bares donde la recogida la efectúa el camarero en nombre de un cliente habitual, o *casas pateras* frecuentados por miembros de la etnia, donde están los encargados de recibir los envíos.

La obtención de los datos de las tarjetas para la realización del fraude, ha sufrido también una evolución importante. Inicialmente se obtenían tarjetas mediante técnicas de *skimming* o copiado de la información de la tarjeta con dispositivos técnicos. Incluso en la red se podían encontrar listados de numeraciones de tarjetas con sus datos de caducidad y titular, aunque la fiabilidad era muy baja porque las entidades bancarias también las observaban en la red y las catalogaban rápidamente de fraudulentas. A día de hoy, los datos de tarjetas se compran en la red a grupos organizados, cuya actividad se centra en la obtención de información financiera de los usuarios, y que más adelante comentaremos.

Las ventas en portales de anuncios clasificados

A medida que la red se ha hecho más participativa, los usuarios han aprovechado las ventajas que ésta les ofrece, y el mundo de las subastas y ventas entre particulares ha experimentado un gran auge. Como no puede ser de otra forma, los delincuentes se han trasladado al nuevo escenario de ventas entre particulares, donde la entrega del producto casi siempre está supeditada a un previo pago, y el fraude se centra sobre las estafas del vendedor hacia el comprador.

Los usuarios ofertan y compran a través de portales web dedicados a ofrecer a los usuarios esta posibilidad. El negocio de los portales está en las pequeñas comisiones que puedan llevarse de cada operación y el derivado de la publicidad. Cuantas más ventas, más rentabilidad para su negocio, por ello, son los primeros interesados en minimizar el impacto

del fraude. Algunos ofrecen sistemas de pago más confiables, como es el caso de eBay con su sistema PayPal, o sistemas de valoración de fiabilidad de vendedores.

El defraudador busca generar el suficiente engaño en la víctima para obligarle a realizar un acto de disposición patrimonial en beneficio del defraudador, es decir, engañarle para que la víctima pague sin haber recibido el producto. El engaño se basa en ofrecer productos estrella con gran demanda, a precios realmente interesantes, y articular un sistema de pago confiable para el pagador.

Los productos estrella en este tipo de fraude son los vehículos de alta gama, las viviendas y el equipamiento informático. Siendo real la venta de coches de segunda mano y de alta gama a precios muy competitivos, los defraudadores se han centrado en ese tipo de ventas. Para ello, aprenden de los anuncios de ventas legales y llegan a copiarlos, para lo que mantienen fluidas comunicaciones con los vendedores y obtienen toda la información necesaria para montar anuncios paralelos de venta del mismo producto, ya sea un vehículo o la venta o alquiler de una vivienda. Los anuncios fraudulentos tienen las mismas fotos, los mismos datos técnicos y las mismas circunstancias del vehículo o la vivienda, incluso copian la identidad del legítimo vendedor, en otra web de anuncios. El engaño se acompaña de situaciones creíbles, como la adjudicación de vehículo de empresa o el desplazamiento por motivos laborales a un tercer país.

Huelga decir que el defraudador se adapta al medio y varía su estrategia conforme ésta es o no rentable y según la tendencia del mercado. Si hoy son coches y casas, ayer eran quads, motos o robots de cocina thermomix, pero siempre acompañan el engaño con suplantación de identidades personales o comerciales.

Un caso particular de tipo de comercio es la venta de productos ilegales o delictivos. Estamos en el caso de venta de titulaciones académicas falsas, licencias de conducir fraudulentas, servicios profesionales de extorsión, amenazas, sicarios, etc. Por supuesto, la mayoría de los servicios y productos ilegales esconden engaños y fraudes al comprador que, por la naturaleza delictiva del producto o servicio, no denunciará.

Los sistemas de pago son los clásicos en el comercio electrónico, la transferencia bancaria o el envío de dinero a través de empre-

sas de transferencia de dinero, tipo Western Union o MoneyGram. En ocasiones, para generar confianza en el comprador, se apoyan en la utilización de falsas empresas intermediarias, que simulen realizar la función de intermediar entre comprador y vendedor para evitar el fraude. Reciben el producto del vendedor y el dinero del comprador, y validan la operación entregando a cada uno lo suyo. Son las empresas llamadas *escrow*. Estas empresas ficticias son creadas virtualmente por los propios estafadores, es decir, son falsas webs que simulan su existencia.

Otra fórmula de engaño es la utilización de falsas empresas de transporte que simulan ser receptoras de la mercancía comprada para obligar a la víctima a abonar su importe. En este caso tampoco son empresas reales, sino websites que simulan su existencia.

Como se ha comentado, alguno de los portales de ventas entre particulares utiliza el sistema de pago por PayPal, que básicamente consiste en cuentas virtuales vinculadas a tarjetas de crédito reales.

La utilización de cuentas bancarias o de tarjetas de crédito vinculadas a cuentas de Paypal, para recibir los pagos, suponen un punto vulnerable para los defraudadores, que quedarían identificados como titulares de las cuentas o tarjetas de crédito. Para ello cuentan con colaboradores financieros, conocidos por el nombre de *mulas*, para recaudar las ganancias, y cuyo único cometido es ofrecer sus cuentas para recibir el dinero y retirarlo inmediatamente para transferirlo a su destinatario final mediante las empresas de transferencia de dinero.

La estructura recaudatoria basada en colaboradores financieros ofrece muchas variantes, y como quiera que se utiliza en otras modalidades de fraude, se desarrollará más adelante.

Un elemento común de estos fraudes es la transnacionalidad de las operaciones. Las operaciones fraudulentas más importantes se realizan entre clientes y vendedores de distintos países, y el dinero circula también entre distintos países, lo que dificulta la persecución.

Vemos pues que hay un desarrollo informático más o menos complejo, con creación de empresas ficticias, que hay una fase de preparación de los fraudes con la recogida de información para copiarla, que hay un estudio de los escenarios más rentables, que hay una técnica y modus operandi que van repitiendo en distintos escenarios o portales de anuncios clasificados, que operan a nivel internacional y que disponen

de red de colaboradores y de un sistema estudiado de recaudación. La utilización de estas técnicas, como es de suponer, evidencia una mayor complejidad, propia de bandas organizadas.

Es difícil precisar cuántas bandas organizadas se dedican a esta actividad, puesto que las actuaciones policiales han sido pocas, y, por la naturaleza del fraude, con una pluralidad de afectados inicialmente desconexos entre sí. Pero casi todas las investigaciones apuntan a unos elementos comunes. La tipología de fraude está liderada por bandas organizadas de rumanos. Estas bandas tienen sus raíces en comunidades o localidades de Rumanía, donde se encuentra la cabeza de la organización delictiva y donde hacen gran ostentación de su poderío económico. En ocasiones, esta ostentación, la divulgan por internet, difundiendo imágenes de sus fiestas, que más parecen orgías en hoteles de gran lujo, y con el uso de vehículos de alta gama. La red de recaudación basada en colaboradores financieros se nutre de inmigrantes de Rumanía, captados normalmente por contactos personales entre los miembros de la comunidad inmigrante. Se profesionalizan para estos cometidos, subsistiendo de esa actividad y abandonando toda actividad laboral legal. Utilizan documentaciones falsas que facilitan la apertura de varias cuentas bancarias para recibir los pagos de las ventas fraudulentas, dificultando su identificación y localización en el terreno.

Una peculiaridad de estos grupos, probablemente debida a la presión de la policía rumana en el control de las transacciones a través de Western Union, es que utilizan mensajeros para la recaudación y control de sus *mulas*, en lugar de remitir el dinero por la empresa de transferencia de fondos.

Por último, señalar una variante, también explotada por las mismas bandas organizadas, en las ventas en portales de anuncios clasificados, dirigido del comprador hacia el vendedor, el de los *honorarios adelantados*. El defraudador compra un producto abonándolo con un talón bancario de importe superior a la compra, con la exigencia de compromiso para el vendedor de abonar la diferencia, a través de empresas de transferencia de dinero. Cuando el vendedor recibe el talón, lo ingresa en su cuenta figurando el abono y sin fijarse que se encuentra retenido a la espera de validación del talón, operativa que lleva varios días. En este periodo, el vendedor remite el producto y la cantidad sobrante del talón, que posteriormente le será descontado de su cuenta por no tener fondos.

Fraude en banca electrónica

El servicio de banca electrónica que ofrecen las entidades bancarias a sus clientes, supone comodidad e inmediatez en las gestiones para los usuarios que hacen uso de él, pero presenta una vulnerabilidad importante, la autenticación del usuario. Inicialmente, los usuarios se identificaban con un sistema de autenticación primario, es decir, con algo que se sabe, un login y un password, un nombre de usuario y una contraseña. Si ésta es conocida por terceros, pueden usurpar nuestra identidad y realizar toda aquella operativa que el banco ofrezca. Ese fue el inicio del fraude bancario.

Los estafadores enviaron correos electrónicos a multitud de usuarios, simulando proceder de la entidad bancaria y requiriendo la conexión al banco para actualizar las contraseñas. Se alegaban motivos técnicos, motivos de seguridad, o actualizaciones de sistemas, y los mensajes incluían enlaces a la supuesta web bancaria. Activando esos enlaces se acudía a una web idéntica a la del banco pero fraudulenta, donde el usuario consignaba sus datos identificativos, su identidad online, que pasaban a poder de los defraudadores, quienes posteriormente accedían a la página original del banco, usurpaban la identidad de la víctima y ordenaban transferencias de dinero a cuentas bancarias bajo su control. Este engaño para hacerse con los datos de identidad online de la banca electrónica se bautizó como *phishing*. El origen del término no está claro. Parece ser que podría provenir del término inglés *fishing*, alusivo a la «pesca» de contraseñas. Otros barajan como origen del término el acrónimo de *password harvesting fishing* (cosecha y pesca de contraseñas). Por extensión, el defraudador que practica el *phishing*, será el *phisher*.

Un error bastante extendido es confundir una parte con el todo. *Phishing* es únicamente la técnica para obtener las contraseñas que nos permiten autenticarnos, y otra es utilizarlas contra el sistema de banca electrónica, usurpando la identidad de su legítimo titular para disponer de su dinero. Y es conveniente recalcarlo porque el *phishing* ya no sólo se practica para obtener las contraseñas de banca electrónica, sino para obtener todo tipo de contraseñas y datos personales, con finalidad defraudatoria o no.

Este fraude, al igual que ocurre en algunas de las modalidades del fraude en el comercio electrónico, precisa la colaboración necesaria de los llamados colaboradores financieros o usuarios que ponen sus cuen-

tas a disposición de los defraudadores para recibir el dinero e inmediatamente retirarlo y entregarlo al estafador, antes de que la víctima se aperciba de la estafa y ordene su devolución. A estos colaboradores financieros se les conoce como *mulas*, nombre también utilizado en otras figuras delictivas como el blanqueo de capitales. El nombre hace alusión al animal de carga necesario para el porte de mercancías, sin más responsabilidad que la carga y fácilmente reemplazable.

Así, el *phisher* que suplanta la identidad de una víctima, ordena transferencias de dinero a la cuenta bancaria de la *mula*, quien recibe aviso inmediato y ha de acudir a la oficina o sucursal bancaria para hacer efectivo el dinero y remitirlo por una empresa de transferencia de dinero al *phisher*.

Este fraude inicialmente tuvo una incidencia muy alta, quizá porque pilló desprevenidos a los bancos, que finalmente reaccionaron, incrementando las medidas de seguridad, y a las policías, que vieron cómo desde cualquier rincón del mundo se suplantaban identidades, generando múltiples víctimas que diversificaban la acción judicial, y a las que se les quitaba el dinero de sus cuentas y, con un sistema rápido, se dirigía el dinero hacia países del este, donde la colaboración policial era más precaria.

En torno a esta actividad se detectaron numerosos grupos que actuaban internacionalmente, remitiendo los mensajes desde ordenadores comprometidos e inseguros que los *hackers* se encargan de localizar, controlar y utilizar para sus fines delictivos, y creando redes de colaboradores financieros, recolectores de dinero o *mulas* cuya misión era remitir el dinero hacia los países del este. Prácticamente en todos los países europeos de la ex república soviética se remitía dinero, lo que permite intuir el volumen de fraude que hubo. El número de fraudes era tan alto y tanta la dispersión de hechos que no se era capaz de vincular las acciones a un mismo grupo, toda vez que actuaban sobre usuarios de distintas entidades bancarias y distintos países.

Otro problema que se detectó en torno a este fraude es el tráfico de datos personales. Hasta la fecha, los usuarios sufrían el spam o correo masivo no deseado con fines comerciales, algo que preocupaba más a las operadoras de internet, por el consumo de red que suponía, que al usuario, que no veía amenazada su intimidad con ello. Pero esos mismos datos que se vendían para el spam, se venden para convertirnos en destinatarios del *phishing*.

Ante el alarmante crecimiento del fraude en banca electrónica, desde la prensa, la banca y la policía se alertó, con profusión, a los ciudadanos, lográndose minimizar su impacto. El ciudadano estaba más atento a los engaños de suplantación de identidad de las entidades bancarias para robarle los datos de identificación del servicio de banca electrónica. Y, como se ha dicho, la banca reforzó el sistema de autenticación con un segundo nivel de seguridad, algo que se tiene. Ya no sólo se identificaba al usuario con algo que sabía, un login y un password, sino que se le efectuaba una pregunta cuya respuesta venía en algo que el usuario debía tener, una tarjeta con coordenadas numéricas o un *token* o testigo que entrega el banco al cliente.

Pero siguiendo la espiral de acción reacción, los *phishers* idearon nuevos métodos para hacerse con las contraseñas o identidad online de sus víctimas. La experiencia de los *hackers* fue vital para esta etapa. De la creación de los virus y gusanos que buscaban causar daño en los sistemas se pasa a diseñar otro tipo de programas que pretenden acceder al sistema y robar información, sin que el usuario sea consciente de ellos. Empieza la industria del malware o software malicioso.

Primero fueron los troyanos bancarios tipo *keylogger*, programas que permiten la captura de pulsaciones de teclado del usuario. Se instalaban en los ordenadores de las víctimas y cuando tecleaban la palabra banco o similar empezaba a capturar las pulsaciones de teclado, sabedores de que entre ellas estaban los identificadores del usuario. La contramedida bancaria fue el diseño de teclados virtuales en pantalla, donde el usuario no pulsaba teclas sino pulsaba clics de ratón en un teclado que aparecía en pantalla. Los *phishers* diseñaron troyanos que capturaban las secuencias de pantalla.

A medida que las entidades bancarias adoptaban medidas preventivas y de seguridad, los phishers ideaban y mejoraban el software malicioso, logrando la sofisticación de los troyanos con técnicas mucho más complejas, que permitían, una vez autenticado el usuario con su banco, establecer una comunicación entre el banco y *phisher* oculta para la víctima. Y así se continúa en una escalada de medidas y contramedidas, combinándolo con la «ingeniería social» o capacidad de engaños que atesoran los estafadores en general.

Esta escalada ha dado lugar a variantes del *phishing* que han adquirido nombre propio:

- *Pharming*, técnica de *phishing* que consiste en derivar las conexiones a banca electrónica actuando sobre los servidores de resolu-

ción de nombres de dominio o DNS. En esencia consiste en que cuando al navegador web se le indica una dirección web de un banco concreto, en vez de acudir al banco adecuado acude a la que el *pharmer* le ha indicado. Esta resolución falsa de nombres de dominio, que lleva a la víctima a la página web falsa, se puede hacer en «local», actuando sobre el propio ordenador de la víctima a través de un programa malicioso, o en «red», actuando sobre los servidores de DNS, ordenadores que están en la red con la función de indicar el «camino» adecuado para acceder a las páginas web solicitadas.

- *Vishing*, técnica basada en la tecnología de *Voz sobre IP* (VoIP) que permite hablar por teléfono a través de la red de Internet. Se manipulan ordenadores para que actúen como auténticas centralitas telefónicas, dando una respuesta similar a una central de banco, a través de la cual solicitan al usuario víctima los datos de identidad bancaria o datos de tarjetas de crédito. La forma de inducir al usuario a que efectúe llamada al número de telefonía por VoIP es mediante el envío de mensajes SMS en los que alerta de gastos no realizados, incluyendo en el mensaje el supuesto número para reclamaciones, que no es otro que el de la centralita de VoIP.
- *Smishing*, o *phishing* a través de mensajes SMS de telefonía móvil. Se realiza un spam de SMS supuestamente remitidos desde la entidad bancaria reclamando respuesta por esa misma vía de datos bancarios.
- *Whaling* o *whale phishing* (*phishing* de ballenas). Es una variante de *phishing* mucho más preparada y dirigida a altos ejecutivos, políticos o empresarios a los que se supone que tienen disponibilidad de cantidades más altas de dinero o manejan información más sensible, y por ellos son objetivos más rentables.
- *Hishing* o *hardware phishing*. Es el *phishing* a través de productos hardware que se comercializan con una vulnerabilidad que permite el acceso fácil al equipo de la víctima o que el propio hardware lleva incorporado en su *firmware* el programa malicioso que permite el robo de información bancaria y su remisión a un servidor bajo control de *phisher*.

Como se puede observar, las variantes son muchas y conjugadas con el ingenio y la capacidad de engaño, con la ingeniería social, las posibilidades de sufrir engaño son muy altas. A modo de ejemplo, por su originalidad, citar dos originales casos de *phishing*. Uno mediante el

envío de un mensaje de correo electrónico presuntamente procedente de la policía de Brasil en que se le indica que está siendo requerido en una investigación policial, para lo que se solicita que acceda a la página web de la policía y conteste a un formulario requerido, estando el enlace en el propio mensaje. Al acceder al mensaje y rellenar el formulario uno es infectado por un troyano bancario. Y el segundo mediante el envío de un SMS informando que ha sido dado de alta en un chat erótico pornográfico, informando que si desea darse de baja debe conectarse a una URL que figura en el mensaje. Al conectarse y solicitar la baja, también se infecta con un troyano bancario.

Qué duda cabe que cuanto más sofisticadas sean las medidas y contramedidas, menor incidencia tiene el fraude, y que siempre serán más vulnerables aquellos que menos medidas de seguridad implementen. Hoy nos movemos en niveles de fraude en banca electrónica altos, y por desgracia no declarados. Prácticamente es una política común de las entidades bancarias asumir el fraude por la propia entidad, descargando a sus clientes de culpa. Esto les lleva, por norma general, a ocultar los datos reales para no perjudicar la imagen institucional. Y si los consumados no son declarados, las tentativas, que son muchísimas más, tampoco lo son. Los sistemas bancarios, en la espiral de acción reacción que mantienen con los delincuentes, han desarrollado sistema de detección de operativas fraudulenta como mejor sistema para evitar el fraude, alcanzándose niveles de eficacia altos.

Un elemento a tener en cuenta en la práctica totalidad de la amplia casuística del *phishing* es la existencia de sistemas informáticos donde se recoge la información de las víctimas. Quien cae en el engaño del enlace a una web fraudulenta, al igual que la víctima del troyano, remite la información personal a un sistema informático ubicado en la red y controlado por el *phisher*. Esto ha obligado a los *phishers* a crear una red de máquinas u ordenadores comprometidos para uso propio, y dispersos por todo el mundo. Nos podemos encontrar que un día la información se manda a un equipo alojado en EE.UU y mañana, a otro distinto situado en Rusia. Los informes hablan que el país con mayor número de páginas alojadas es Estados Unidos, seguido de Rusia. La existencia de estos servidores y de las páginas fraudulentas o *fakes* de bancos es uno de los indicadores del nivel de fraude que hay en torno al *phishing*. Las entidades bancarias contratan servicios informáticos de empresas dedicadas a neutralizar, en el menor tiempo posible, las páginas que afectan a su entidad. Por otro lado, la acción policial contra este tipo de fraude,

dista mucho de ser eficaz, toda vez que como se ha podido intuir, por la complejidad de su realización y la diversidad de actores que participan, está monopolizada por bandas organizadas, que operan a nivel transnacional, haciendo muy difícil su persecución.

Si a la escasa eficacia de las actuaciones policiales se suma la pasividad de las entidades bancarias a denunciar tanto los hechos consumados como el enorme volumen de tentativas de fraude existentes, por temor a consecuencias negativas a la imagen institucional o del servicio de banca electrónica, se está creando un espacio de impunidad para el delincuente que favorece el crecimiento de este tipo de delitos.

Vemos pues que es un modelo delictivo muy estructurado en el que hay desarrolladores con altos conocimientos técnicos, utilización de recursos de red, estructuras de blanqueo de dinero a través de *mulas*, y los organizadores del fraude. Y además, creciente por la escasa presión que sufren. Por ello, y en base a estimaciones de volumen de fraude, se comenta que la industria del crimen que rodea al fraude en banca electrónica está creciendo a pasos agigantados, llegando a ser más rentable que otras actividades clásicas de la delincuencia organizada, como el tráfico de drogas. Lo que sí se ha observado es que el crecimiento está trayendo consigo la especialización de las funciones, creándose grupos dedicados a sólo alguna de las etapas o pasos del fraude en banca electrónica y ofreciendo su especialización como servicio para otras bandas delictivas. Es el crimen como servicio, *crime as a service*.

Crime as a service

El crecimiento del *phishing*, derivado de la rentabilidad del delito, tanto en criterios económicos como de impunidad, hace proliferar los grupos organizados que aterrizan en este escenario delictivo. Un escenario que precisa de desarrollos informáticos para el diseño de falsas páginas web de entidades financieras, de malware para infectar las máquinas y controlarlas, y para obtener información de éstas.

El incremento de grupos en torno al *phishing* les obliga a buscar, entre los ambientes *hackers*, gente capaz de cubrir sus necesidades. Qué duda cabe que la demanda trae consigo el incremento de la oferta, y ésta deriva en un abaratamiento de los costes de los productos o desarrollos informáticos. En el entorno del mundo *hacker*, a través de foros o canales temáticos de fraude se empieza a comercializar las herramientas de *phishing*, los troyanos que roban información de las víctimas.

Por otro lado, debido a la permanente respuesta del mundo de la seguridad informática y bancaria, el *hacker* está obligado a una constante innovación. Todo el malware que desarrolla tiene una vida limitada hasta que es descubierto. Pero no sólo el malware, sino las técnicas de hacking para detectar agujeros de seguridad o bugs en los sistemas o programas, que permiten acceder sin ser detectados, tienen una vigencia hasta que el desarrollador del software corrige el error. Esta actividad creativa ha alcanzado cotas insospechadas, llegándose a una producción de malware sin precedentes, donde las empresas de seguridad antimalware, no son capaces de dar una respuesta eficiente.

Dentro de este mundo del malware, fruto de los análisis que llevan a cabo las empresas antivirus y otras del sector, se pueden definir dos corrientes o escuelas. La de los países del este y la de los brasileños. La primera tiene su influencia o campo de acción sobre los usuarios europeos y norteamericanos, y la segunda sobre los latinoamericanos. Pero el efecto globalizador de la red también se deja notar en ambas escuelas, donde se empieza a detectar que unas copian de otras. Tras los recientes incidentes de Google con *hackers* chinos, se empieza a hablar también de la escuela china, no tan orientada al fraude de banca electrónica sino al robo de información.

Consecuencia de esta amplia actividad de desarrollo de malware, las bandas organizadas empiezan a dejar de tener *hackers* a su servicio, para empezar a contratar servicios que éstos venden. Y el *hacker*, de esta forma, se desvincula del hecho delictivo concreto y sólo ofrece el instrumento. El más claro ejemplo de esto es la venta de kits de *phishing* en la que un usuario cualquiera, sin conocimientos avanzados de informática puede adquirir en el mercado del malware, un kit que sólo ha de configurar y poner en funcionamiento, para empezar a infectar equipos y obtener información de sus usuarios. Incluso en los acuerdos de servicio por el kit, informan que el desarrollador no se hace responsable del mal uso del programa.

Lamentablemente la cultura de seguridad informática es muy escasa, tanto a nivel doméstico como a nivel empresarial. La informática es concebida como un servicio y no como un activo que requiere de una inversión en seguridad. Consecuencia de esto es la ausencia o insuficiente dedicación de esfuerzos a la seguridad de los equipos y sistemas, y el gran número de máquinas y servidores susceptibles de ser comprometidos.

Existen numerosos estudios, la mayoría de ellos realizados por las empresas del sector de la seguridad informática, que arrojan cifras escalofriantes. En España, el Instituto Nacional de Tecnologías de la Comunicación (INTECO), ha realizado diversos estudios del estado de la sociedad de la información en el escenario español. Muchos de los resultados son extrapolables a la sociedad global. Por ello, es de recomendada lectura el *Estudio sobre la seguridad de la información y eConfianza de los hogares españoles* y el *Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas,* al que ya se ha hecho mención al inicio del presente capítulo. En el último estudio publicado se habla de que, prácticamente dos de cada tres equipos domésticos, está infectado con malware.

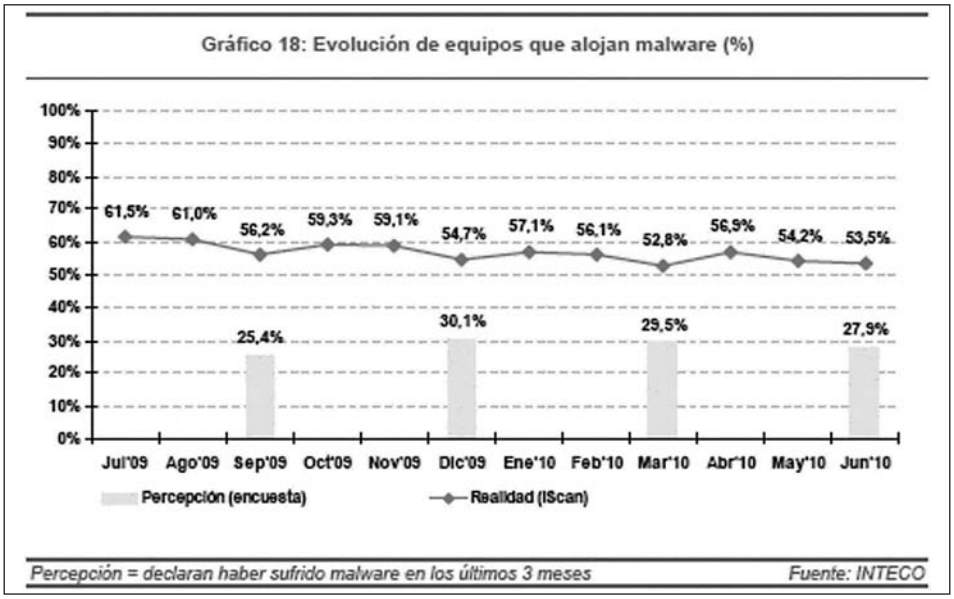


Figura 1. Gráfico de evolución de equipos que alojan malware. Fuente: INTECO.

Los *hackers* son conscientes de esta realidad y de las posibilidades que ello supone. El valor de los sistemas no está en el sistema en sí, sino en la información que almacenan. Si se es capaz de entrar en un sistema ajeno, aprovechando vulnerabilidades o deficiencias de configuración, y controlarlo remotamente, o se es capaz de infectar un ordenador con un troyano para robar la información bancaria, también se puede infectar para entrar y robar cualquier tipo de información o espiar la actividad y comunicaciones del usuario.

Así, el malware que diseña sirve para más funciones. Ya no sólo es troyano bancario para espiar los datos de conexión a banca electrónica, sino que permite el control del ordenador, roba las contraseñas de los accesos a los distintos servicios que tenga el usuario, ya sea su webmail, su cuenta de PayPal, la cuenta del casino virtual o las contraseñas de banca electrónica.

De esta forma el *hacker*, va conformando una legión de ordenadores infectados, bajo su control, a los que les puede robar la información y ordenarles que realicen cualquier acción, ya sea conectarse a una web determinada, mandar un mail o borrar su propio disco duro, es decir, crear su propia red de ordenadores zombis, red de robots o *botnet*, como se le conoce en el argot *hacker*.

Siguiendo la política de disminuir riesgos y responsabilidades, algunos *hackers* capaces de desarrollar este software, en lugar de utilizarlo, lo ponen a la venta, comercializándolo como un servicio personalizable. Otros, sin embargo, lo explotan y lo que comercializan es la información que obtiene.

Así, se ha creado un mercado negro de información personal de todo tipo, pero especialmente de datos financieros. Podemos encontrar que se están vendiendo filiaciones de personas completas, con números de tarjetas de identidad, seguro médico, y todo lo necesario para fingir en la red ser otro; y podemos también encontrar listado de tarjetas de crédito con todos los datos necesarios, ordenados por entidades bancarias y por saldo disponible, con todos los datos necesarios para su operativa. En fin toda la información que guardemos en nuestros sistemas y que puede ser robada, puede ser vendida. Es el comercio de los datos personales.

Pero una red de ordenadores bajo control de un *hacker* tiene más posibilidades. Pueden utilizarlos para realizar ataques contra terceros; pueden convertir los equipos en repositorios de malware, de música, de películas, e incluso de pornografía infantil; pueden utilizarlos para enviar *spam*, pueden causar daños en los equipos, borrando cualquier tipo de información o programa, y pueden utilizar los equipos para cualquier actividad de fraude.

Dentro de los ataques a terceros cabe mención especial los ataques a la disponibilidad de la información o bloqueo de los sistemas. Si cuando el usuario requiere el uso del sistema o de la información, no está disponible por la acción de terceros, nos enfrentamos a una denegación

de servicio (DoS del inglés Denial of service). Muchas empresas, tienen como única línea de negocio, la prestación de un servicio a través de la red. Otras, sin ser la única línea de negocio, su funcionalidad es parte de la imagen empresarial. Imaginemos las consecuencias para un banco que no pudiera prestar el servicio de banca electrónica por la acción de terceros sobre los sistemas informáticos del banco.

Relacionado con los ataques DoS, hay que mencionar el *black mail*. Las bandas organizadas ya se han hecho eco del riesgo que supone para algunas empresas la disponibilidad de sus sistemas y han actuado al más puro estilo mafioso, exigiendo sumas de dinero, extorsionando, para que sus sistemas no sufran ataques de «denegación de servicio».

Y nuevamente esta potencialidad de las *botnes*, frente a la demanda del mundo del crimen, se empieza a ofrecer como servicio. Se alquilan las *botnets*.

Otro elemento imprescindible para la ejecución del fraude en banca electrónica es la existencia de equipos u ordenadores deslocalizados por la red, donde almacenar la información y las *fakes* de los supuestos bancos. Para ello se desarrollan herramientas que exploren la red en busca de servidores mal configurados o vulnerables a determinados fallos de seguridad, que permitan la instalación de sistemas de control remoto. También se buscan servidores que garanticen el anonimato de sus usuarios gracias a legislaciones que no obligan a guardar los datos de registro de sucesos de los sistemas, es decir, servidores en paraísos informáticos.

En torno a esta necesidad se han creado auténticas infraestructuras de servidores e incluso de proveedores de servicio de internet (ISP), que conscientes de que sus clientes hacen un uso delictivo de él, y amparados en una normativa inexistente o deficiente, prefieren mantener una estructura de red que les genera beneficios. Fue especialmente famosa la RBN (Russian Business Network) constituida por un conjunto de ISP que ampararon en un momento determinado la gran mayoría del fraude de banca electrónica que existía.

La infraestructura de mulas

A lo largo de las distintas estructuras organizativas de la delincuencia que se ha creado en torno al cibercrimen, se ha comentado la necesidad del blanqueo de las ganancias procedentes del delito, utilizando

colaboradores financieros o *mulas*. El tema se ha descrito de forma muy generalista y como indicio determinante del carácter organizado de la delincuencia que recurre a este sistema de blanqueo y recaudación de las ganancias del delito. Y se ha dicho que como elemento común de varios tipos de delitos se describirá con más detalle. Vistos los fraudes y la industria del malware, llega su turno.

La tipología de *mulas* es muy diversa y ha sufrido una evolución significativa. En los inicios, las bandas organizadas enviaban a los distintos países donde operaban personal de la banda con varias identidades falsas y con cada una de ellas y en distintas entidades y sucursales abrían cuentas bancarias para recibir el dinero de las víctimas.

Posteriormente, trasladaron a miembros de la banda como captadores de *mulas* entre colectivos de inmigrantes naturales de los países donde se ubicaba la cabeza de la banda organizada. Buscaban el apoyo de sus paisanos, sabedores de que éstos eran conscientes de los riesgos que corrían si eludían o intentaban apoderarse de las ganancias que debían trasladar. Dada la escasez de recursos económicos de los inmigrantes y el escaso reproche penal que sufrían si eran objeto de la acción policial y judicial, les era fácil encontrar personas dispuestas a hacer de *muleros*. Los captadores se dedicaban a ofrecer pingües ganancias a quienes están dispuestos a colaborar, dándoles las instrucciones oportunas incluso para hacer frente a la acción policial, con coartadas creíbles, como la recepción de ingresos procedentes de herencias de amigos de su país remitidas para evitar la acción fiscal de su gobierno, o ingresos procedentes de separaciones matrimoniales de amigos para evitar el control del cónyuge.

También se captaban *mulas* vinculadas al mundo de la droga que estaban dispuestas a ofrecer sus cuentas por las escasas ganancias que les permitirán adquirir nuevas dosis de droga. Hasta mujeres de países del este, víctimas del tráfico de seres humanos para la prostitución, traídas bajo engaño a nuestro país y obligadas a la prostitución para pagar su presunta deuda, retirándoles su identidad con la que abrían cuentas corrientes para recibir los ingresos de victimas de *phishing*.

El endurecimiento de la acción judicial, con sentencias calificando la acción de las *mulas* de cooperación necesaria, obligó a las bandas organizadas a agudizar el ingenio para captar nuevas *mulas*, toda vez que la vida útil de éstas, en la inmensa mayoría de los casos es de una sola recepción de dinero procedente del fraude.

Sin dejar de coexistir los anteriores procedimientos de captación de *mulas*, a día de hoy, el sistema de captación de *mulas* ha migrado hacia el engaño, siendo éste el más utilizado. Remiten mensajes de correo electrónico a multitud de usuarios proponiendo una colaboración financiera para una empresa que va a empezar a operar en el país. Las ganancias son porcentuales en función de lo que reciba en su cuenta, y aseguran que se puede llegar a ganar cantidades de hasta 3.000 €con dedicación exclusiva. La cobertura de las empresas es muy diversa y muchas de ellas creíbles, como el caso de la agencia matrimonial de mujeres de países del este, que se desplazan al país de la «*mula*» y cuando contraen matrimonio, el supuesto cónyuge abona los servicios a través de ingresos al colaborador financiero o *mula*. Es de suponer que, según el grado cultural de la *mula*, hay consciencia o no de su vinculación al mundo del delito. Pero lo cierto es que los delincuentes agudizan el ingenio y crean historias que pueden llevar al engaño a cualquiera. Actualmente y con la crisis económica que atenaza a prácticamente a todos los países, son técnicas habituales el reclutar *mulas* con distintos engaños entre los usuarios de portales de empleo.

A ello hay que sumar la reciente normativa europea de creación de la Zona Única de Pagos en Euros, conocida bajo el acrónico de SEPA (de la terminología inglesa Single Euro Payments Area), que establece la liberación de las transferencias internacionales electrónicas, con lo que el dinero objeto del fraude, ya sean de banca electrónica o de comercio electrónico, se transfiere libremente de un país a otro, dificultando aún más la acción policial y judicial. Las *mulas* españolas empiezan a recibir el dinero procedente de fraudes cuyas víctimas se hallan en terceros países europeos, y viceversa.

Tal es la actividad de captación de *mulas* mediante las técnicas de engaño, que se ha creado en torno a él redes de delincuentes especializados en el tema, capaces de diseñar engaños, acompañados de la infraestructura tecnológica necesaria, como son páginas web simulando empresas o negocios legales, capaces de obtener listados de usuarios que concurren, aportando sus currículos, a portales de trabajo, y capaces de lanzar campañas dirigidas a estos usuarios seleccionados para el engaño, que la función de captación de *mulas*, también se empieza a ofrecer como servicio para el mundo del crimen organizado.

Por último, hay que tener presente que la función de la *mula* no es otra que recibir el dinero, procedente del fraude, en su cuenta corriente

y remitirlo, previa comunicación, vía empresa de transferencia de dinero, a un tercer destinatario. Como ya se ha comentado en anteriores apartados, el fraude en la red que se sufre en el espacio europeo proviene mayoritariamente de organizaciones delictivas afincadas y naturales de países del este. Algunas de ellas, especialmente desde que se compartimenta las fases del fraude ofreciéndose como servicio, se afincan en Reino Unido. Por tanto, el dinero debe dirigirse hacia esos destinos. Esto nos obliga a tener en cuenta dos aspectos, que el responsable de las *mulas* ha de ponerse en contacto con la *mula* para indicarle donde ha de enviar el dinero y que el dinero transferido deja un rastro en los operadores de transferencia de fondos.

Las comunicaciones de los responsables con sus *mulas* siempre es telemática. Para ello se utilizan redes que permiten anonimizar las comunicaciones, servidores comprometidos donde se instalan servidores de correo y las clásicas cuentas de servidores webmail anónimos, como Hotmail, Yahoo o Gmail. Esta es otra de las funciones que los grupos organizados dedicados a la captación de *mulas* asumen en su portfolio de servicios.

Para evitar la trazabilidad del rastro del dinero, el sistema de *mulas* también se utiliza en destino. Es decir, la remisión del dinero por las empresas de envío internacional de fondos no es directa al *phisher*, sino que en destino también lo reciben *mulas* que, posteriormente, directamente o a través de un recaudador, lo entregan al *phisher*. Esta diversificación dificulta sobremanera la acción policial incluso contando con la excelente colaboración de las empresas de envío de dinero, sistema legal y muy útil especialmente para los numerosos colectivos que sufren el fenómeno de la inmigración.

Los timos en la red

No podemos finalizar este documento sin hacer referencia a la pequeña delincuencia organizada que se genera en torno a los timos. El concepto de timo, engaño mediante promesa de ganancias fáciles de dinero, ha existido desde siempre en la vida real. Pero para ser víctima de esos engaños, resultaba preciso cruzarse en el camino del timador. Ahora, Internet, nos ha acercado a todos a los timadores. Servicios tan populares como el correo electrónico, utilizados por todos, nos convierten en potenciales víctimas de los timadores que remiten de forma masiva, a modo de *spam*, mensajes con supuestos de importantes ganancias fáciles, que no son otra cosa que burdos engaños para estafarnos.

Quizá el más popular de todos los timos en la red sean las cartas nigerianas. En ellas se alude a supuestas fortunas de ciudadanos africanos que por razones políticas de exilio o de accidentes inesperados, han fallecido dejando su dinero sin un legítimo sucesor o con trabas administrativas para que éstos puedan disponer del dinero. La participación de la víctima se reduce al pago de una pequeña cantidad de dinero en concepto de impuestos, sueldos para comprar a empleados bancarios corruptos o a funcionarios que falsificarán documentos oficiales, convirtiéndole en legítimo destinatario de fortunas que siempre rondan cifras millonarias de dólares. A cambio de esta colaboración los beneficios que se pueden obtener rondan los 10 ó 15 millones de dólares.

En ocasiones los mensajes recibidos con este tipo de fraudes son burdas traducciones del inglés, en las que se evidencia el engaño por todas partes. En otras, tienen una perfecta redacción e incluso son acompañadas de enlaces a webs en los que se hace referencia al fallecimiento o exilio del millonario africano. Lógicamente, estas páginas son falsas, creadas por los propios timadores.

El segundo timo más popular es el de las loterías internacionales, en las que se avisa de la ganancia de un premio millonario. Suelen vincularse a servicios de apuestas existentes, tipo Bonoloto española o europea. La participación del agraciado (timado) está originada por supuestas empresas que, para promocionarse, asocian cuentas de correo electrónico a números que participan en el sorteo. La ganancia siempre está en torno a fortunas de 50 millones de euros y la obligación del premiado es adelantar el pago de tasas o comisiones para la empresa encargada de gestionar los números ganadores. Igual que en el anterior timo, las comunicaciones se adornan con copias de páginas oficiales de los organismos de loterías.

Este tipo de timos están liderados por bandas organizadas de ciudadanos nigerianos, que fueron quienes empezaron con esta actividad con las famosas cartas nigerianas. Por eso, a estos timos también se les conoce como los fraudes del *Scam del 419*, en alusión al número del artículo del código penal nigeriano en que se tipifican los fraudes. Su estructura organizativa está a caballo entre Nigeria, de donde se envían muchos de los mensajes cebo, y Reino Unido y España, donde está el aparato encargado del cobro y de buscar los reclamos necesarios para orquestar los timos.

La incidencia de esta estafa es pequeña y las víctimas se sitúan mayoritariamente entre los ciudadanos americanos y asiáticos, y al igual que con las bandas de subsaharianos, el beneficio es pequeño. Permite

a pequeños grupos organizados subsistir, lo que les lleva a hacer de esta actividad su estilo de vida.

BIBLIOGRAFÍA

FERNÁNDEZ TERUELO Javier Gustavo, *Cibercrimen, los delitos cometidos a través de Internet*, Oviedo, Constitutio Criminalis Carolina, 2007,181.

HERNÁNDEZ GONZÁLEZ Claudio, *Hackers, piratas tecnológicos*, Madrid, Coelma, 1998, 410.

MATA Y MARTIN Ricardo M. «Criminalidad Informática: una introducción al cibercrimen», *Actualidad Penal*, nº 37, 2003, 127.

PANDA SECURITY, *Datos bancarios al descubierto*, publicado en julio de 2009, disponible en [www.pandasecurity.com/img/enc/Boletines%20PandaLabs4.pdf]

PANDA SECURITY, *El Negocio de los Falsos Antivirus*, publicado en julio de 2009, [disponible en

www.pandasecurity.com/img/enc/El%20Negocio%20de%20los%20falsos%20antivirus.pdf]

PANDA SECURITY, *Informe anual año 2009*, publicado en Enero 2010, [disponible en www.pandasecurity.com/img/enc/Informe_Anual_Pandalabs_2009.pdf]

PANDA SECURITY, *Informe trimestral Abril-Junio 2010*, [disponible en www.pandasecurity.com/img/enc/Informe_Trimestral_PandaLabs_T2_2010.pdf]

SANZ MULAS Nieves, *El desafío de la Criminalidad organizada*, Granada, Comares S.L. 2006, 280.

S21sec, *Informe análisis: Apuestas y fraude en Internet 2009, p*ublicado en febrero de 2010, [disponible en www.s21sec.com/descargas/Apuestas_fraude_S21sec.pdf]

S21sec, *Informe especial: Carding y Skimming,* publicado en febrero de 2010

S21sec, *Informe de Fraude Online y Cibercrimen 2005-2009,* [disponible en www.s21sec.com/servicios.aspx?sec=157&apr=202]

SYMANTEC, informe Norton Online Family report 2010

SYMANTEC, Informe Norton Online living report 2009

CAPÍTULO CUARTO

SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN

LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN

NÉSTOR GANUZA ARTILES

RESUMEN

El capítulo IV trata de los riesgos y peligros que amenazan la seguridad de las sociedades modernas debido a su dependencia de las Tecnologías de la Información.

Se introduce al lector en los asuntos de mayor conflictividad dentro del marco internacional de la ciberseguridad; en los dilemas que surgen de la necesidad de proteger las redes y los servicios de información y a su vez proteger las libertades individuales inherentes a sociedades democráticas, en especial la libertad de expresión y la protección de la intimidad.

Se estudian y analizan dos casos de ciberataques de gran transcendencia mundial: los ciberataques cometidos contra Estonia, en la primavera de 2007, conocidos por ser el primer caso en que unas operaciones cibernéticas afectan de manera clara, drástica y global a la seguridad nacional de un país; y los ciberataques cometidos contra Georgia, en el verano de 2008, conocidos por ser el primer caso en el que las operaciones cibernéticas son iniciadas y conducidas conjuntamente con operaciones militares armadas.

Por último se analiza la situación de la ciberseguridad en la OTAN y el proceso de transformación que la OTAN está llevando a cabo en dicha materia.

Palabras clave: Ciberataque, ciberdefensa, ciberseguridad, ciberamenaza, ciberdisuasión, OTAN, NCIRC, CDMA, CCDCOE, Estonia, Georgia, Rusia, DDoS, botnet, investigación forense.

CYBERSECURITY SITUATION IN INTERNATIONAL FIELD AND THE NATO

ABSTRACT

Chapter IV deals with the risks and dangers that threaten the security of modern societies due to its dependency on Information Technology.

It introduces the reader in the most contentious issues within the cyber security international framework, on the dilemmas that arise from the need to protect networks and information services while protecting individual liberties inherent in democratic societies, particularly freedom of expression and privacy.

It is studied and analyzed two cases of cyber attacks of world importance: cyber attacks committed against Estonia, in the spring of 2007, known for being the first case in which cyber operations affect the national security of a country in a clear, dramatic and comprehensive fashion; and cyber attacks committed against Georgia, in the summer of 2008, known as the first case in which the cyber operations are initiated and conducted in conjunction with armed military operations.

Finally we analyze the state of cyber security in NATO and the transformation process that NATO is carrying out in this issue.

Key words: Cyber attack, cyber defense, cyber security, cyber threat, cyber deterrence, NATO, NCIRC, CDMA, CCDCOE, Estonia, Georgia, Russia, DDoS, botnet, forensic investigation.

INTRODUCCIÓN

Tópico es iniciar el tema que nos ocupa subrayando la dependencia de las sociedades modernas y de los países desarrollados de los sistemas de información. En cualquier introducción de cualquier libro relacionado con el tema aparece esta idea como básica para el desarrollo de sus argumentos posteriores, no en vano el desarrollo de la sociedad de la información en los países avanzados es a su vez su gran fortaleza y su gran debilidad.

A pesar de los riesgos que conlleva una sociedad cada vez más interconectada digitalmente y cada vez más olvidada de los procedimientos

tradicionales, la tendencia digital es imparable; lo que significa que hay que afrontar el futuro como es y gestionar los riesgos asociados.

Los riesgos asociados son numerosos, entre los que destacan, una mayor y más compleja actividad criminal desarrollada por grupos organizados o delincuentes individuales; una más prolífica actividad terrorista que hace uso del ciberespacio ampliamente para actividades terroristas y para apoyo a ellas; una mayor y más compleja actividad de espionaje, ya sea industrial, militar o político; una mayor variedad y cantidad de ataques a las infraestructuras críticas nacionales, a las libertades públicas y a todo tipo de servicios en los que se basa el funcionamiento de las sociedades modernas; un mayor índice de ataques camuflados, orquestados por Estados y encubiertos bajo apariencia de ataques con origen en bandas criminales, activistas políticos, etc.; una mayor participación de ciudadanos particulares en acciones maliciosas, ya sea por ignorancia, por curiosidad, por diversión, por reto o por lucro; y un largo etcétera de riesgos como causa de la atracción que el ciberespacio produce al ofrecer una mayor rentabilidad, globalidad, facilidad e impunidad para todo este tipo de actividades.

Como reacción a esta avalancha de amenazas, que en definitiva son amenazas al estado de bienestar y al sistema democrático de los países desarrollados, surge la necesidad de militarizar la red.

La militarización de la red no debe ser entendida como una ocupación de la red por fuerzas militares con el objetivo de controlar los movimientos en ella, sino como el derecho de las naciones a disponer de ciber armamento en defensa de sus legítimos intereses. Nuestros enemigos las poseen y las usan. Un percepción mal entendida que confine la capacidad militar a los medios convencionales nos pondría en una clara y peligrosa situación de desventaja.

El comandante jefe de la Fuerza Aérea Británica, Sir Stephen Dalton, declara en un discurso pronunciado en el Instituto Internacional de Estudios Estratégicos de la Defensa del Reino Unido, que

> *«el crecimiento exponencial de la disponibilidad de medios de información significa que debemos entender cómo distribuir y proteger nuestros intereses nacionales en el dominio cibernético y, aunque se trata claramente de una cuestión de gobierno, la defensa tiene un interés legítimo en el desarrollo de capacidades defensivas y ofensivas cibernéticas. En el futuro nuestros adversarios pueden usar ciberataques contra nuestros sistemas de informa-*

> *ción. De hecho nuestros sistemas informáticos nacionales están, hoy, bajo ataques constantemente. Nuestros enemigos actuales ya están utilizando efectivas operaciones de información y propaganda, a través de Internet, sobre las bajas civiles para tratar de influir en la opinión pública y limitar nuestras actividades. En fin, que van a usar todos los medios posibles a su alcance para tratar de anular nuestra libertad porque entienden que cuando se utiliza con eficacia, es su ventaja comparativa»* (1).

El antiguo Director de la Inteligencia Nacional de los Estados Unidos, Mike McConnell, declara que las ciber armas deben ser consideradas como armas de destrucción masiva (2).

La carrera armamentística cibernética es un hecho (3). Según el experto analista de ciber seguridad Kevin Coleman la carrera comenzó en 2006 con una docena de países participando en su desarrollo y utilización. En 2007, el número de países aumentó en un 450%. Las cyber armas han proliferado en todo el mundo y ahora son parte de los arsenales en 150 países, 30 de los cuales han incorporado unidades cibernéticas dentro de sus ejércitos (4). En la actualidad, se estima que participan en la carrera más de 200 países, grupos terroristas, organizaciones criminales, organizaciones extremistas y facciones de activistas.

El panorama se vuelve más sombrío, dudoso y alarmante cuando se considera que las organizaciones criminales, los grupos extremistas y terroristas también han entrado en la carrera.

Los servicios de inteligencia militar de todo el mundo están tratando de monitorizar el desarrollo y la venta de armas cibernéticas, así como qué de identificar los grupos que están detrás de los ataques cibernéticos. Un gran número de agencias gubernamentales están interesadas

---

(1) Artículo publicado el 16 de febrero de 2010 por «The Independent». http://www.independent.co.uk/news/media/online/twitter-is-a-weapon-in-cyber-warfare-1900535.html

(2) Mr. Mike McConell en una entrevista ofrecida en el programa televisivo «Charlie Rose Show», el 8 de enero de 2009.

(3) Kevin G. Coleman en su informe «el derecho a disponer de ciber armamento» («The right to bear cyber arms». http://www.technolytics.com/Right_to_bear_cyber_arms_CCH9-2.pdf

(4) Kevin G. Coleman, en su artículo «Private Sector-Military Collaboration Vital to Confront Cyber Threats». http://www.defensetech.org/2010/04/19/private-sector-military-colaboration-vital-to-confront-cyber-threats/

en el aprendizaje de las capacidades de las armas cibernéticas y las intenciones de los activistas y extremistas para el uso de tales armas (5).

Sin duda alguna el Ciberespacio debe ser considerado y estudiado para su posible inclusión en la doctrina militar como un espacio de la batalla más, conjuntamente con los espacios de tierra, mar y aire; de tal manera que las operaciones conjuntas dispondrían de un componente más.

En este capítulo se analizará la situación internacional en ciberseguridad a través del estudio de dos casos reales de ciber guerra (Estonia 2007 y Georgia 2008) y a través del análisis de la situación actual en la OTAN.

LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL

La respuesta ante ciber ataques solo es efectiva desde una perspectiva internacional, en donde es vital consolidar acuerdos firmes de colaboración entre Estados, organizaciones o alianzas militares internacionales, el sector privado, la industria y el sector académico.

Maeve Dion, investigadora del Centro de Protección de Infraestructuras Críticas de la Universidad de George Mason en los Estados Unidos, advierte del peligro de conflicto en el área de ciberseguridad entre la OTAN y la Unión Europea, por la diferente prioridad que dichas organizaciones establecen en sus programas relacionados con la materia y esto a la larga es fuente de problemas para los países pertenecientes a ambas organizaciones (6).

A su vez en la respuesta deben tomar parte diferentes actores que hablan diferentes lenguajes, por lo que es necesario trabajar de manera concienzuda en la coordinación multidisciplinar en los campos científico, tecnológico, político, diplomático, económico, jurídico, militar y de inteligencia.

El ruido legal alrededor del mundo cibernético no hace más que favorecer los intereses de ciertos países y de grupos criminales y terroristas que les conviene un cierto grado de ambigüedad jurídica para situarse en una posición de ventaja sobre los países democráticos, en los que las libertades públicas y los derechos de expresión y privacidad, entre otros,

(5) Op.Cit. 3

(6) Maeve Dion, en el prefacio del libro «International Cyber Incidents, legal considerations». Eneken Tikk, Kadri Kaska y Liis Vihul, publications@ccdcoe.org

hace que las fuerzas armadas y las fuerzas del orden y seguridad tengan muchas restricciones a la hora de hacer uso del ciberespacio.

Valga de ejemplo, el uso casi tabú que se hace del término «ciber ataque» en los entornos políticos y militares de los países democráticos, haciéndose uso de eufemismos tales como «ciber defensa activa».

Las múltiples líneas borrosas que surcan el ciberespacio como, el uso legal de equipos de penetración (red team), el uso legal de monitorización de las redes, el uso legal de datos personales para investigaciones forense de ciber ataques (7), la determinación de las fronteras nacionales y la integridad territorial en el ciber espacio, la atribución legal de ciber ataques, las competencias policiales y militares, etc; no hacen más que beneficiar a potenciales enemigos y adversarios que hacen uso de las armas cibernéticas para atacar a sociedades democráticas que a su vez cuestionan el uso de las mismas armas para defender sus intereses.

Sin ir más lejos, todas las actividades educativas y ejercicios en la OTAN relacionados con el hecho cibernético son de ciber «defensa». Existe una duda moral y legal en ciertos sectores de si se puede instruir y entrenar a militares en el uso de herramientas de ciber ataque, ya que dicha formación les puede servir para realizar acciones delictivas privadas sin el control de los propios ejércitos.

Como si esto fuera un caso distinto a la instrucción y entrenamiento con armas de fuego, esencia de los ejércitos y que también pueden ser usadas a posteriori para cometer delitos sin el control de los propios ejércitos.

La formación de unidades militares específicas de ciberguerra no es más que la obligación que tienen los ejércitos de adaptar sus funciones a las tecnologías del momento, como en su día se hizo con la incorporación de las unidades de misiles, NBQ (8) o guerra electrónica.

Otro tema de discusión en el ámbito internacional acerca de la ciber seguridad es el concepto de «disuasión cibernética». ¿Cómo lograr una efectiva disuasión ante ciber ataques?

La disuasión se entiende como la firme intención y predisposición de un Estado víctima de un ataque de causarle al atacante un daño mayor del sufrido en justa represalia y en legítima defensa. La disuasión tiene

(7) Por ejemplo, es actualmente debatido en países desarrollados si la dirección IP es dato personal o no.

(8) NBQ: Nuclear, bacteriológico y químico.

como objetivo persuadir a los atacantes de llevar a cabo sus malévolas intenciones. Es una manera efectiva de prevención.

En la disuasión cibernética, a diferencia de en la nuclear, el principal problema consiste en ¿cómo amenazar y prevenir un atacante que se desconoce?. En la disuasión nuclear el atacante deja su firma instantes después de lanzar un ataque nuclear, en la disuasión cibernética, en muchos casos no es posible saber con exactitud quién es el originador, responsable u organizador de los ciber ataques. Además, en los pocos casos que es posible una identificación cierta, ésta se logra después de meses de trabajo forense y la reacción del Estado víctima ya no es inmediata y la legítima defensa podría no ser un argumento válido.

Por otro lado, en la mayoría de los casos, los ciber ataques se basan en atacar desde multitud de puntos dispersos por el globo a unos pocos puntos concretos de la víctima. La represalia inmediata no es posible, puesto que atacar a los atacantes no surtiría efecto por la imposibilidad de la concentración de objetivos y por la duda de si el atacante realizó el ataque deliberadamente o su infraestructura fue secuestrada sin su conocimiento.

El concepto de disuasión en el ciberespacio debe cambiar totalmente su filosofía y basarse en la prevención, en hacer al atacante no rentable el ataque y en una sólida colaboración internacional y no en una represalia instantánea.

Para finalizar este apartado valga una reflexión sobre el uso del ciberespacio por parte de los terroristas.

En primer lugar, los terroristas necesitan que sus acciones sean lo suficientemente graves como para mantener atemorizada a una determinada sociedad durante un tiempo relativamente largo; y para ello nada mejor que un atentado con daños o posibilidad de daños físicos graves o mortales a personas. En este caso, el ciber espacio es un terreno todavía por explorar por los grupos terroristas más influyentes, que fundamentalmente usan la red como plataforma de apoyo logístico, de comunicaciones, de reclutamiento y propagandística.

En segundo lugar, los terroristas necesitan de un gran aparato mediático que de publicidad a sus acciones de la manera más rápida y extensa posible. En este caso los terroristas no tienen que esforzarse mucho, ya se encargan los propios medios de comunicaciones de los países democráticos, en donde la libertad de información está garantizada, de hacerles esa función y el ciberespacio garantiza su cobertura a nivel mundial.

EL CIBER CASO ESTONIA 2007

Antecedentes

En la primavera de 2007 el gobierno de la República de Estonia anuncia su decisión de realizar excavaciones en la plaza de Tonismäe, con motivo de encontrar restos de soldados caídos durante la segunda guerra mundial enterrados en el subsuelo y posteriormente identificarlos y enterrarlos en el cementerio militar de Tallin.

La decisión del gobierno incluía el traslado y emplazamiento, de forma permanente, de la estatua conocida como «el soldado de bronce» (9) a la entrada del mencionado cementerio militar.

El soldado de bronce es considerado por la «comunidad rusa» en Tallin (10) como un símbolo de sus caídos en la segunda guerra mundial y es costumbre depositar flores a sus pies en señaladas fechas conmemorativas de la victoria rusa. Por el contrario para la «comunidad estonia» el soldado es considerado como un símbolo de la era soviética que trae no buenos recuerdos a muchos estonios. Según Rain Ottis (11), para la minoría local rusa el soldado representa al «libertador» mientras que para los estonios representa al «opresor».

La situación que se vivía era de normalidad; la comunidad rusa utilizaba la plaza y el monumento como lugar de celebración en fechas señaladas y los estonios toleraban los actos sin darle más importancia.

Pero la situación cambió el 9 de mayo de 2006 cuando la policía tuvo que intervenir en una trifulca entre miembros de la comunidad rusa que

---

(9) El soldado de bronce es un monumento instalado en la mencionada plaza en 1947 con motivo de la conmemoración de la victoria del ejército soviético sobre el ejército alemán durante la segunda guerra mundial. En 1947 Estonia formaba parte de la extinta Unión Soviética bajo régimen de Stalin.

(10) Según el Registro de Población hasta el 1 de enero de 2009, 1.364.100 personas viven en Estonia, en representación de más de 100 etnias diferentes. Los principales grupos étnicos son: estonios (68,6%), rusos (25,6%), ucranianos (2,1%), bielorrusos (1,2%) y finlandeses (0,8%). Según el Censo de Población del año 2000, en Estonia se hablan 109 lenguas. El 83,4% de los ciudadanos estonios habla estonio como lengua materna, el 15,3%, ruso, y el 1% restante habla algún otro idioma. Datos extraídos de la Embajada de Estonia en Madrid. http://www.estemb.es/estonia/integracion

(11) Rain Ottis, experto en Ciber seguridad que formó parte del equipo encargado por el gobierno estonio de planificar y ejecutar la respuesta a los ciber ataques sufridos por Estonia en 2007, en su informe «Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. (9)

portaban banderas de la extinta Unión de Republicas Socialistas Soviéticas y estonios que portaban banderas de la República de Estonia –entre partidarios pro-kremlin y movimientos nacionalistas estonios–. A partir de este hecho la sociedad estonia se fue polarizando cada vez más y el soldado de bronce se convirtió en el punto de encuentro de manifestantes extremistas, cada vez más con mayor agitación; de tal manera que la plaza a partir de entonces tuvo una vigilancia especial por parte de la Policía.

Con la sociedad cada vez más polarizada, animada por la prensa local y por la prensa rusa, y con manifestaciones nacionalistas localizadas alrededor de un símbolo con dos significados enfrentados; el debate en la sociedad estonia estaba servido (12), ¿Por qué no trasladar el símbolo de un lugar céntrico y emblemático de la ciudad a una zona más apartada donde las manifestaciones no tengan tanta visibilidad y repercusión?

Así que el gobierno estonio anunció su decisión del traslado a principios de la primavera de 2007 y el 26 de abril de 2007 comenzaron los trabajos preparatorios. Este hecho provocó una manifestación, seguida de actos vandálicos sin precedentes en Estonia por el número de participantes, por la violencia de sus actos, por el número de arrestados –1.300– y por el número de heridos –cientos–, incluyendo un muerto. Para encontrar un hecho de similar magnitud en Estonia, hay remontarse a los disturbios provocados por la Fuerza Aérea Soviética en 1944 y la anterior ocasión en que como consecuencia de disturbios callejeros en Tallin hay víctimas mortales hay que remontarse a 1918.

Estos disturbios fueron conocidos como «la noche de los cristales«. En concreto, en la mañana del 26 de abril de 2007, numerosas personas se congregaron de manera pacífica en la plaza del soldado de bronce para protestar por la decisión del gobierno de trasladar el monumento, pero por la tarde se unió un grupo con una actitud violenta, el cual se enfrentó a la policía y horas más tarde comenzaron actos vandálicos por la ciudad, rompiendo escaparates. La policía no tomó el control de la situación hasta el siguiente día, el 27 de abril de 2007.

---

(12) Hay que considerar que la sociedad estonia no está habituada a desordenes públicos, manifestaciones, huelgas, etc. El autor de este capítulo lleva viviendo en Estonia desde Julio de 2008 sin haber presenciado, o tenido noticia alguna, a través de amigos y compañeros o a través de medios de comunicación de ninguna manifestación, protesta pública o huelga.

El 27 de abril de 2007 mientras proseguían los enfrentamientos callejeros entre la policía y grupos violentos de la comunidad rusa, varios hechos significativos surgieron simultáneamente:

a) comenzaron los ciber ataques a sistemas de información de la infraestructura pública y privada estonia.

b) los medios de comunicación locales, nacionales e internacionales se hacían eco de la situación con desigual puntos de vista.

El ICDS (13) declara que la gran mayoría de la prensa nacional e internacional informó fehacientemente de los hechos incluyendo los actos vandálicos y los destrozos producidos a establecimientos y negocios. Por el contrario, los medios de comunicación rusos no informaron sobre el vandalismo y enfocaron la noticia como un acto de violencia ejercido por la policía estonia contra pacíficos manifestantes. Lo cual fue un perfecto caldo de cultivo para diversos artículos agresivos contra Estonia y su forma de resolver el asunto, incluyendo unas declaraciones de un parlamentario ruso que consideró el acto como causa de guerra (14).

El Baltic News Services (15) y el Postimees (16) informan sobre hechos que inducen a pensar en la implicación de la Embajada rusa en Tallin en la organización de los actos vandálicos de la noche de los cristales.

En concreto el Baltic News en su edición del 25 de abril de 2007 informa acerca de reuniones sostenidas repetidamente entre Sergei Overtshenko, consejero de la embajada rusa y Dmitri Linter leader de la «Patrulla Nocturna», grupo sospechoso de llevar a cabo los actos vandálicos durante la noche de los cristales.

El Baltic News en su edición de 18 de abril de 2007 y el Postimees en su edición de 25 de abril de 2007 informan acerca de la reunión sostenida el 18 de abril de 2007 entre Andrei Zarenkov, líder del Partido Constitucional Estonio, y firme defensor del soldado de bronce y Vadim Vassilyev, primer secretario de la embajada rusa. Posteriormente a la reunión, el mismo día, Zarenkov anunció que la jefatura del Partido Constitucional Estonio ha decidido reclutar agitadores voluntarios con la misión

(13) ICDS: International Centre of Defence Studies. www.icds.ee.

(14) «Russia's involvement in the Tallinn disturbances», 12.05.2007, a compact overview compiled by the ICDS. www.icds.ee.

(15) Ibid

(16) Ibid

de convencer a los militares estonios que la intervención de las Fuerzas Armadas Estonias en el conflicto sería inaceptable.

c) comenzaron las acciones de movimientos juveniles, en especial el movimiento «Nashi» (17), las más destacables: el bloqueo de la embajada estonia en Moscú y la agresión a la embajadora durante una conferencia de prensa.

Según el ICDS hay suficientes datos para afirmar que el Kremlin está directamente relacionado con la organización y decisión del bloqueo de la embajada estonia en Moscú (18).

Según el «Eesti Päevaleht»(19) en su edición del 2 de mayo de 2007 el bloqueo se caracterizó por unos aspectos que no suelen coincidir en una manifestación pública espontánea; como que los participantes en el bloqueo disponían de un autobús para prepararse las comidas, de 30 tiendas de campañas exactamente iguales, de modernos dispensadores de agua, equipos de sonido, pancartas de material de gran calidad que se cambiaban cada día, etc.

Pero el hecho incuestionable es que la embajada estuvo asediada durante una semana (del 27 de abril al 1 de mayo), impidiendo el normal desarrollo de entradas y salidas del recinto, incluyendo a la embajadora Marina Kaljurand y el Vice-Cónsul Silver Laanemäe, sin que la policía remediara la intolerable situación.

La evidencia más clara de la implicación del kremlin en el asedio se deriva de una conversación telefónica mantenida por el Ministro de Asuntos Exteriores de la Federación Rusa Yevgeny Primakov con su homólogo alemán Frank-Walter Steinmeier, sacada a la luz por «The Financial Times, Germany» el 5 de mayo de 2007, en la que el ministro ruso aseguraba que el gobierno de la federación rusa se aseguraría de que la policía forzara la finalización del bloqueo bajo una condición, que la embajadora estonia abandonara Moscú.

El hecho es que el mismo día que la embajadora abandonó Moscú, los bloqueadores levantaron el bloqueo y la policía las barreras de protección.

---

(17) Nashi: es un movimiento de jóvenes políticos en Rusia, que declara ser movimiento democrático antifascista.

(18) Op. Cit.7

(19) http://www.epl.ee/

Es claro para el autor que los ciber ataques no fueron un hecho aislado sino que estaban enmarcados dentro de una situación política claramente definida, en la que hay considerar además el poco agrado que causo en el kremlin la adhesión de Estonia a la OTAN en 2004. El grado de implicación de las autoridades rusas en el conflicto, en las manifestaciones y actos vandálicos en Tallinn y en el bloqueo y acoso a la embajada y embajadora en Moscú es difícil de determinar, pero existen multitud de datos que apoyan la tesis de que los enfrentamientos no fueron espontáneos sino que contaron con la complicidad de las autoridades rusas.

Cronología de los ciber ataques

Los ciberataques a Estonia tuvieron lugar entre el 27 de abril y el 18 de mayo de 2007, a.i. Durante este periodo los ataques variaron su objetivo, volumen y método, pero en líneas generales se pueden distinguir dos fases principales:

Fase 1, del 27 al 29 de abril, en donde los ataques debida a la inmediatez del conflicto tenían un componente emocional y esto en sí mismo constituía la motivación para unirse a los ciberataques y como todo acto emocional eran básicamente de naturaleza simple, es decir, sin grandes complejidades de carácter técnico y organizativo y sin capacidad de convocar a un número de atacantes lo suficientemente grande como para causar daños serios y poner en una situación de crisis o indefensión a Estonia.

Según Lauri Alman(20), la primera fase se caracterizó por el uso de herramientas de ciber ataque rudimentarias y simples, llevados a cabo por hacktivistas (21) sin grandes conocimientos técnicos, los cuales hacían uso de herramientas que a su disposición se emplazaban en sitios web, rusos mayoritariamente, conjuntamente con las correspondientes instrucciones (22). Las herramientas estaban especialmente diseñadas para atacar sitios web de Estonia y especialmente del gobierno, del ministerio de Defensa y de los principales partidos políticos.

(20) Lauri Alman, durante el conflicto era el Secretario de Estado de Defensa de Estonia y formaba parte del comité de crisis formado para la ocasión.

(21) Ver glosario

(22) Lauri Alman en la entrevista ofrecida a Wyatt Kash para GCN (www.gcn.com) el 13 de junio de 2008. http://gcn.com/articles/2008/06/13/lauri-almann--lessons-from-the-cyberattacks-on-estonia.aspx

El primer ataque, registrado e informado(23), relacionado con el caso Estonia fue contra sitios web gubernamentales durante la noche del 27 de abril de 2007(24).

En concreto, cuenta Laury Alman que miembros del gobierno estonio se encontraban en una reunión en la sala de situación del gobierno cuando el responsable jefe de relaciones públicas entra en la sala y comenta que no eran capaces de cargar los comunicados de prensa en los sitios web oficiales del gobierno, los miembros del gobierno allí presentes no le dieron más importancia hasta que fueron advertidos expresamente que estaban bajo ciber ataque, esto ocurrió la noche del 27 al 28 de abril de 2010 a la 01 de la mañana (25).

Una vez confirmado que el país estaba bajo ciber ataque el gobierno procedió de manera inmediata a organizar un equipo de respuesta liderado y coordinado por el Equipo Nacional de Respuesta ante Incidentes Informáticos (Estonian CERT)(26) y compuesto por personal experto de los ministerios de Comercio y Comunicaciones, y de Defensa, así como de los servicios de Inteligencia.

Este fue un gran triunfo de Estonia: *identificar la gravedad del asunto con celeridad y organizar inmediatamente un equipo de respuesta multidisciplinar e investirle de la autoridad necesaria.*

Fase 2, del 30 de abril al 18 de mayo, en donde el conflicto en las calles se difumina trasladándose al ciber espacio, donde los ánimos de los ciudadanos de Estonia (rusos y estonios) se calman y no hay lugar para ataques emocionales, en esta situación más fría los ataques se volvieron más complejos tanto en el aspecto técnico como en el organizativo y en la coordinación; sucediéndose ataques mucho más sofisticados que necesitaban de un mayor conocimiento de las herramientas de ciber guerra, al menos por parte de los organizadores y de un uso de grandes «botnets»(27) y de una coordinación minuciosa y precisa.

---

(23) Es importante recalcar esto, «ataque informado», porque en muchos casos los ataques recibidos por entidades importantes son silenciados por miedo a perdida de reputación, fiabilidad o fidelidad de los clientes.

(24) Op. cit., 13

(25) Ibid.

(26) CERT: Computer Emergency Response Team.

(27) Una botnet es una red formado ordenadores secuestrados o infectados –robots informáticos o bots–, que ejecutan tareas de manera autónoma y automática y que normalmente pasan desapercibidas para el legítimo propietario o usuario. El Centro

Los sitios web usados en la primera fase que sirvieron de plataforma de lanzamiento de ataques seguían en funcionamiento en esta segunda, pero con mejoras añadidas, como listas de objetivos y calendario en los que se indicaba hora y lugar del ataque para conseguir un enorme volumen de peticiones simultáneas sobre los mismos servicios informáticos con el fin de dejarlos fuera de servicio (28).

Una de las características más interesantes de esta fase es la relación existente entre la situación política y los ciberataques. Como ejemplo más revelador, valga destacar, el espectacular incremento de los ataques coincidiendo con la fiesta nacional rusa conmemorativa de la victoria sobre el ejército alemán en la segunda guerra mundial, esto es el 9 de mayo de 2007. El incremento fue del 150% a las 11 horas de la noche (hora local estonia) del 8 de mayo que coincide con el comienzo de la fiesta nacional en Moscú (00.00 horas del 9 de mayo, hora de Moscú).

Según José Nazario (29), se registraron 21 ataques de denegación de servicios distribuidos (DDoS (30)) durante el 3 de mayo de 2007, 17 durante el 4 de mayo, 31 durante el 08 de mayo, 58 durante el 09 de mayo y 1 durante el 11 de mayo (31).

Tipos de ataques

Los tipos de ataques llevados a cabo en el caso Estonia fueron principalmente los siguientes:

a) Ataques de denegación de servicios (DoS)

El ataque de denegación de servicio es un ataque informático que utiliza el protocolo TCP/IP para conseguir que un determinado servicio o recurso prestado por un sistema de información sea inaccesible a los usuarios legítimos. El ataque se puede realizar desde un solo punto o desde muchos puntos simultáneamente.

---

de Mando y Control de la Botnet puede controlar todos los ordenadores o servidores infectados de forma remota.

(28) Rain Ottis, overview of events, 02 de mayo de 2007, CCDCOE activation team, TDCCIS

(29) José Nazario es un destacado analistas de ciber amenazas a nivel mundial, forma parte del equipo de Arbor Networks. http://asert.arbornetworks.com/authors.php#authID8

(30) DDoS: ver glosario.

(31) José Nazario, Arbor Networks, 17 de mayo de 2007. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

Cuando el ataque procede desde muchos puntos simultáneamente, generalmente haciendo uso de Botnets, se denomina «ataque distribuido de denegación de servicio» (DDoS).

En general, se necesita un número muy grande de atacantes ejerciendo peticiones de servicio simultáneamente sobre un mismo objetivo para conseguir la perdida de conectividad de la red de la victima por el consumo de su ancho de banda o sobrecarga de los recursos computacionales.

Son varias las maneras de congregar un número grande de atacantes sobre un mismo objetivo simultáneamente, entre las que se destacan:

– La propaganda: como en la primera fase del caso Estonia, se motiva emocionalmente a potenciales atacantes y se les da instrucciones precisas y apoyo técnico para sus acciones. Este es el caso básico, pero con resultados normalmente mitigables por la dificultad de congregar un número suficiente para causar daño.
– A través de botnets: secuestrando recursos computacionales de personas o entidades que normalmente desconocen su aportación, y controlando dichos recursos desde un punto origen –Centro de Mando y Control de la Botnet–.
– A través de granjas de servidores (32): ya sea usando granjas de servidores asociadas a instituciones estatales, o alquilándolas en el sector privado.
– Una combinación cualquiera de las tres anteriores.

En el caso Estonia, los métodos más usados fueron DDoS mediante «inundación ICMP (33)», «inundación UDP (34)» y peticiones deforma-

(32) Granja de Servidores: es un grupo interconectado de servidores que sirve para ejecutar tareas que necesitan de una gran capacidad computacional.

(33) Inundación ICMP (ICMP flood) consiste básicamente en el envío masivo y continuado de peticiones ping (peticiones mediante paquetes ICMP Echo que tratan de comprobar la accesibilidad de una determinada entidad de la red) a un solo objetivo, obligando a la víctima a responder a todas las peticiones ping (con paquetes ICMP Echo reply, pong) respuesta en. Si el desequilibrio entre número de peticiones y la capacidad de respuesta de la víctima es grande se produce una sobrecarga de la red y del sistema de la víctima.

(34) Inundación UDP (UDP flood): consiste básicamente en el envío masivo y continuado de peticiones UDP (el protocolo UDP no necesita de conexión previa, ni tiene confirmación de errores. Es usado fundamentalmente en servicios de audio y de video en tiempo real). Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP Spoofing.

das y con menos intensidad «inundación SYN (35)» y el «ping de la muerte (36)».

Se sospecha que además de botnets secuestradas se usaron también botnets y granjas de servidores de alquiler, pero no se ha podido comprobar hasta la fecha.

Según Linnar Viik (37) los últimos ataques no fueron realizados a través de redes de ordenadores zombis si no a través de algo que no se puede comprar en el mercado negro –en alusión a una intervención estatal organizada–, una capacidad estatal de ciber guerra y esto es algo que debe ser profundamente analizado pues constituye un nuevo nivel de riesgo. En el siglo 21 la competencia de un estado no es sólo su territorio y su espacio aéreo sino además su infraestructura electrónica (ciber espacio) (38).

José Nazario contabilizó 128 ataques de denegación de servicio durante el periodo comprendido entre el 03 y el 11 de mayo, de entre los cuales, 115 usaron el método de inundación ICMP y 10 consumieron 90 Mbps durante 10 horas, por lo que deduce que «*alguien está muy, pero que muy empeñado en causar daño a Estonia y este tipo de cosas se incrementarán en los próximos años*» (39).

b) Ataques de desfiguración de sitios web (web site defacement)

El ataque de desfiguración de web es un ataque mediante el cual se accede a un sitio web clandestinamente con el objetivo de modificar el aspecto visual.

---

(35) Inundación SYN (SYN flood) consiste básicamente en el envío masivo de peticiones de conexión (paquetes TCP/SYN) a un solo objetivo. El objetivo atacado trata cada uno de los paquetes recibidos como una petición de conexión y responde con paquete TCP/SYN-ACK para establecer la conexión y se mantiene a la espera de la respuesta del supuesto peticionario (paquete TCP/ACK). La respuesta nunca llega porque la petición es falsa y todo esto consume la capacidad del servidor e impide que dé respuesta a peticiones legítimas.

(36) Ping de la muerte (Death ping): consiste básicamente en el envío masivo de paquetes ICMP muy pesados (mayores a 65.535 bytes) con el objetivo de colapsar el sistema atacado. Es un ataque que aprovechaba una vulnerabilidad de los sistemas operativos anteriores a 1998, por lo que este ataque fue efectivo solo en unos pocos casos muy determinados.

(37) Linnar Vikk, durante el caso Estonia era asesor del gobierno en materia de tecnología de la información.

(38) Linnar Vikk en un aartículo de Peter Finn para el Washington Post, 19 de mayo de 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

(39) Op. cit. 22

En el caso Estonia se realizaron ataques de este tipo fundamentalmente a sitios web oficiales modificando los contenidos originales por otros de carácter apologético de la causa rusa y en lengua rusa.

Uno de los principales objetivos en estos ataques fue el primer ministro de Estonia Andrus Ansip. En uno de estos ataques los hackers modificaron el contenido del sitio web del partido político del primer ministro y entre otras cosas emplazaron una fotografía de Andrus Ansip con bigote tipo Hitler.

c) Ataques a servidores de sistemas de nombres de dominio

Un sistema de nombres de dominio es un sistema jerárquico que asocia información variada con nombres de dominios asignados a cada uno de los participantes en servicios o recursos conectados a internet o a una red privada. Su función más importante, es traducir nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, con el propósito de poder localizar y direccionar estos equipos mundialmente.

Un ataque de este tipo es tremendamente peligroso pues el servidor DNS es una pieza fundamental e indispensable para el funcionamiento de internet.

En el caso Estonia, en las webs que servían de apoyo a los atacantes no avezados en las tecnologías de la información se daban instrucciones de cómo atacar DNS conjuntamente con las direcciones IP y URL de objetivos. Los DNS destacados como objetivos en las webs maliciosas fueron el servidor DNS nacional –administrador de los nombres de dominio de la administración pública–; el EENet –administrador de los nombres de dominio de la red de servidores de las instituciones del Gobierno y de Educación– y los DNS de proveedores estonios de servicio de internet (40).

d) Correo basura (spam)

Correo basura son aquellos mensajes de correo electrónico que se reciben sin haberlo solicitado, sin permiso o autorización del receptor, habitualmente no deseados y de remitentes desconocidos. En la ma-

(40) Eneken Tikk, Kadri Kaska y Liis Vihul, International Cyber Incidents, legal considerations. ccdcoe@ccdcoe.org (3)

yoría de los casos con finalidad publicitaria. Cuando el correo basura se recibe en grandes cantidades puede llegar a ser molesto para el receptor.

En el caso Estonia, no hablamos de correo de carácter publicitario molesto para el receptor, sino de ataques bien organizados basados en el envío masivo de correos electrónicos generados por robots a direcciones oficiales gubernamentales y direcciones privadas de personajes relevantes de la política estonia.

Este tipo de ataque es más sencillo y efectivo de lo habitual si se realiza contra un país como Estonia, debido a la política de transparencia cibernética que el gobierno estonio impulsa desde 2001 y que obliga a publicar todas las direcciones de correo electrónico y webs de todos los servicios públicos. Una vez más la democracia y las libertades públicas juegan un papel en favor de los «malos».

Objetivos

El tipo de objetivos es una evidencia de que los ataques no fueron espontáneos y fueron meticulosamente estudiados para conseguir una mayor daño a nivel político, económico, comercial y de comunicaciones y en definitiva de pérdida de confianza y reputación de un país que tiene por orgullo ser uno de los países más comprometidos con la tecnología de la información y la ciber sociedad (41).

(41) Datos extraídos de http://estonia.eu/about-estonia/economy-a-it/economy-at-a-glance.html que dan idea de la vinculación de Estonia con la ciber sociedad:
- 76% de la población de 16 a 74 años son usuarios de Internet (2010, Estadísticas de Estonia).
- 63% de los hogares tiene acceso a Internet (2009, Estadísticas de Estonia).
- Todas las escuelas de Estonia están conectados a Internet.
- Todas las ciudades de Estonia y los pueblos están cubiertos por la red de puntos públicos de acceso a Internet.
- Hay más de 1100 zonas de Internet inalámbrico gratuito en todo el país. Más información: www.wifi.ee
- Los ingresos pueden ser declarados a la Administración Aduanera y Tributaria a través de Internet. En 2010, el porcentaje de declaraciones de impuestos electrónicas fue del 92%.
- Los gastos efectuados en el presupuesto general del Estado se pueden seguir en Internet en tiempo real.
- El Gobierno ha cambiado las reuniones del gabinete por sesiones sin soporte de papel mediante un sistema de documentación basado en web.
- Todo el territorio de Estonia tiene garantizada la cobertura de telefonía móvil digital.

Los objetivos políticos más atacados fueron las webs, redes y servicios del gobierno, primer ministro, presidente de la república, parlamento, oficina de estudios estatales, ministerios, policía y partido política del gobierno.

Estonia es un país donde la actividad política, –y me refiero al trabajo propio de los políticos en el desempeño de sus funciones–, se realiza mayoritariamente a través de sistemas de las tecnologías de la información. Las sesiones del gobierno y los consejos de ministros se realizan exclusivamente a través de intranet, evitando casi al 100% la burocracia del papel. Un ataque con éxito a las redes que controlan dicha actividad provocan de inmediato una crisis de comunicación política.

Los objetivos económicos estuvieron enfocados principalmente en los servicios de e-banking de los principales bancos nacionales, Hansapank y SEB Eeesti Uhispank. Estonia ofrece un perfil adecuado para facilitar a un ciber atacante el estudio y la decisión de los objetivos financieros: los dos bancos mencionados controlan el 80% del mercado bancario nacional con lo que se facilita la concentración de los ataques y los ciudadanos estonios hacen uso mayoritariamente de los servicios bancarios a través de internet –del orden del 90% de todas las transacciones bancarias se realizan electrónicamente– con lo que el daño está asegurado.

A día de hoy las entidades bancarias afectadas no han hecho públicas las pérdidas sufridas debido a los ciber ataques.

A los daños producidos por los ciber ataques hay que añadir los daños comerciales debido al cierre de la frontera de la Federación Rusa a transportes de gran tonelaje procedentes de Estonia, coincidiendo en tiempo con los ciber ataques. Otra evidencia del interés de la Federación Rusa en causar daño a Estonia.

Los objetivos de comunicaciones se enfocaron en los proveedores de servicios de internet más importantes, Elion, Elisa y Starman; en los administradores de servicios de nombres de dominio, DNS Nacional, EEnet y en los medios electrónicos de comunicación más influyentes: Postimees, Delfi, EPL y Baltic News.

En definitiva Estonia reunía una serie de requisitos que la hacían altamente atractiva para sufrir un ciber ataque masivo por parte de su vecino, la Federación Rusa, principal sospechoso de instigar y organizar los ataques:

1. La entrada de Estonia en la OTAN no fue vista con muy buenos ojos por parte de su vecino. El «soldado de bronce» es una excusa perfecta y elemento catalizador para iniciar un conflicto con un país no amigo con ánimo de causar daño (42).
2. Estonia es un país con una dependencia grande de las tecnologías de la información con lo que un ciber ataque puede ser una buena elección si se quiere causar mucho daño sin obtener a cambio ninguna baja, perjuicio o imputación legal.
3. Estonia es un país de dimensiones reducidas (43) y perteneciente a la OTAN, con lo que un ciber ataque masivo puede dar lugar a una situación de crisis de seguridad nacional y así de paso comprobar y estudiar la fortaleza y la capacidad cibernética de las alianzas internacionales.

   Ene Ergma (44), portavoz del parlamento estonio, declara «Estonia es un estado miembro de la OTAN, un ataque a Estonia es una manera de comprobar las defensas de la Alianza. Los atacantes pueden examinar la capacidad de respuesta de la OTAN bajo la tapadera del conflicto «soldado de bronce». Cuando observo una explosión nuclear y la explosión sucedida en mi país en mayo, veo la misma cosa, como la radiación atómica, la ciber guerra no hace sangre pero lo destruye todo» (45).

La respuesta técnica

La respuesta técnica a los ataques fue variada, básicamente el proceso fue el siguiente: primero, se eliminaron las funcionalidades de los servicios web para ahorrar ancho de banda, segundo se solicitó más ancho de banda al proveedor y finalmente se cortaron las conexiones con el extranjero.

El 30 de abril de 2007 el gobierno estonio bloqueó el tráfico de internet procedente de Rusia, filtrando todas las direcciones con extensión «punto ru» (.ru). Al día siguiente los proveedores de servicios de internet

(42) Op. Cit. 14.

(43) Estonia tiene una superficie de 45.228 km2, similar a la extensión de la comunidad autónoma de Aragón (47.720 km2) y una población de 1.340.415 habitantes, inferior al municipio de Barcelona (1.621.537). www.estonia.eu.

(44) Ene Ergma, científica y política, doctora por el Instituto Ruso de Investigación Espacial. Portavoz del parlamento estonio.

(45) Ene Ergma en una entrevista concedida a Josua Devis para wired.com. http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia#ixzz10MKnJXOC

de Estonia se vieron forzados a suspender el servicio a todos los clientes durante medio minuto para poder reinicializar las redes (46).

Como ejemplo significativo valga comentar el caso del Postimees (47), el periódico electrónico de más tirada en Estonia(48). Ago Väärsi, editor jefe, descubrió el 28 de abril de 2010 que sus servidores de páginas estaban inundados de peticiones (más de 2,3 millones) y quedaron fuera de servicio más de 20 veces. Habitualmente la capacidad no usada de los servidores es de un 30 %, por lo que la capacidad de los servidores mantienen un margen de seguridad para demandas extras, pero en este día la capacidad no usada de los servidores empezó a caer drásticamente, 20%, 10%, 5%, 0%, el sitio web es inaccesible por saturación.

El correo no deseado –spam– sobrecargaba los servidores y se come todo el ancho de banda; Väärsi elimina la funcionalidad de comentarios para ahorrar ancho de banda, pero los atacantes variaban sus formas de ataques y mantenían fuera de servicio a los servidores.

Ante nuevos ataques Väärsi estaba preparado, no solo había eliminado la posibilidad de comentarios sino que había hecho las páginas mucho más ligeras eliminando la publicidad y las fotografías, pero los servidores seguían fuera de juego.

Se vio obligado a solicitar un aumento de ancho de banda a su proveedor Elion, pero con 110 Mbps, el máximo disponible, no era suficiente para mantener los servidores operativos.

Inmerso en el estudio de la situación, descubre que la mayoría de peticiones de acceso procedían de Egipto, seguido por Vietnam y Perú –evidentemente no era debido a un repentino interés de los egipcios, vietnamitas o peruanos en la vida social de Estonia o en la lengua estonia–, por lo que decidió cortar la conexión con el extranjero. El ancho de banda se recuperó inmediatamente, el servicio comenzó a funcionar pero sólo en Estonia, el periódico no podía informar al mundo de lo que estaba pasando. Batalla perdida.

La misma medida de cortar la conexión con el extranjero fue tomada por bancos y organizaciones gubernamentales.

---

(46) Peter Finn en un artículo en el Washington Post, 19 de mayo de 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

(47) www.pstimees.ee

(48) En Estonia el 40 % de la población lee el periódico diariamente por internet.

Hillar Aarelaid, el jefe del equipo nacional de respuesta ante incidentes informáticos (CERT), fue encargado por el gobierno de Estonia de la coordinación de la respuesta en el conflicto, pero el CERT estonio no tiene más capacidad para hacer frente a grandes botnets dispersadas por el globo que la de desconectar a Estonia del resto del mundo.

La lucha contra las botnets requiere una defensa basada en una coordinación internacional. Aarelaid necesitaba del apoyo de influyentes personalidades con capacidad de tomar decisiones sobre la conectividad de internet a nivel mundial. A tal efecto se reunió, el 8 de mayo de 2007, con Kurtis Lindqvist, Patrick Fälstrom y Bill Woodcock (USA).

Inmediatamente, Aarelaid y su equipo comenzaron examinar el tráfico para descubrir las fuentes originales de los ataques. Entre otros hallazgos encontraron una botnet, compuesta por ordenadores situados en los EE.UU. que habían sido secuestrados.

Pero la respuesta técnica es claramente insuficiente. Lauri Alman comenta como ejemplo, que cuando empezaron a anular botnets con la ayuda de la Unión Europea y de los Estados Unidos, los administradores de las botnets fueron lo suficientemente astutos como para trasladar las botnets a jurisdicciones menos amigables o menos desarrolladas jurídicamente, de tal manera que la cooperación con Estonia no era posible (49).

Después del ataque, Estonia toma una serie de medidas técnicas encaminadas a fortalecer la capacidad de prevención y respuesta ante incidentes informáticos, entre las cabe destacar, fortalecer la infraestructura vertebral de Internet (backbone), ampliar las conexiones con la «World Wide Web» para que la capacidad en Internet sea más difícil de desbordar, integrar todos los servicios electrónicos del gobierno en un solo sistema centralizado (X-Road) y ampliar e invertir aún más en la capacidad de detectar ataques cibernéticos.

La respuesta política

En general, las naciones aisladamente no tienen capacidad para hacer frente a ciber ataques masivos cometidos a través de botnets dispersadas por el mundo.

(49) Op.Cit. 14

Las naciones no tienen capacidad técnica para ejecutar acciones sobre el tráfico de internet que circula por redes que físicamente se encuentran fuera de su territorio y no tienen competencia jurídica para imponer sus leyes fuera de su jurisdicción; por lo tanto sólo y exclusivamente desde la cooperación internacional se puede abordar el problema.

Relevantes son las palabras del Presidente de la República de Estonia en su discurso del 24 de septiembre de 2010 en la asamblea general de las Naciones Unidas, en el que recuerda que para hacer frente a los desafíos de seguridad del siglo veintiuno, es indispensable la cooperación exitosa entre todos los estados, organizaciones internacionales y regionales; y en este sentido, las amenazas informáticas no son una excepción; e insta a la construcción de una capacidad amplia transfronteriza e intersectorial para la protección de las infraestructuras críticas de información. La necesidad de una cooperación más estrecha entre los Estados, el sector privado y la sociedad civil es urgente ya que en caso de un ataque cibernético, todas las medidas tradicionales de seguridad podrían ser inútiles (50).

El apoyo internacional en Estonia fue organizado por el Ministro de Defensa, quién inmediatamente puso en conocimiento de la situación a sus aliados de la OTAN y de la Unión Europea.

Era claro que el artículo 4 (51) del Tratado de Washington, respaldaba a Estonia para requerir una consulta formal de los estados miembros de la OTAN, por considerar el conflicto como un caso que afectaba a la seguridad nacional y a la independencia política.

Pero el requerimiento de la aplicación del artículo 5(52) del Tratado era un paso de tuerca más que debía ser cuidadosamente meditado y

---

(50) Toomas Hendrik Ilves, presidente de la república de Estonia, en su discurso en la asamblea general de las Naciones Unidas, New York 24-09-2010. http://president.ee/en/speeches/speeches.php?arhiiv=2010

(51) Tratado de Washington, 4 de abril de 1949, **artículo 4**. Las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada.

(52) Tratado de Washington, 4 de abril de 1949, **artículo 5**. Las Partes acuerdan que un *ataque armado* contra una o más de ellas, que tenga lugar en Europa o en América del Norte, ser considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudar a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas

finalmente fue descartado, según se desprende de las palabras que en su día pronunció el Ministro de Defensa estonio, «en estos momentos la OTAN no define claramente el ciber ataque como una acción militar…, ningún ministro de defensa de un estado miembro definiría un ciber ataque como una acción militar a día de hoy (53)».

En un primer momento, Estonia obtuvo la cooperación de sus aliados en la Unión Europea y Estados Unidos para anular botnets; seguidamente con la ayuda de sus aliados aumentó su capacidad en internet (ancho de banda, troughput) pero tuvo que hacerlo gradualmente y sin revelar la capacidad real, debido a que la red era constantemente monitorizada por los atacantes para, entre otras cosas, tener información puntual del ancho de banda de la infraestructura nacional estonia y modificar sus ataques de acuerdo con la inteligencia obtenida.

Observadores de los CERTS nacionales de los Estados Unidos y de la OTAN visitaron Estonia durante el 8 y 10 de mayo para observar de primera mano la situación y dar apoyo técnico. El CERT nacional de Finlandia fue especialmente útil para llevar a cabo la coordinación internacional entre CERTs nacionales.

El simple hecho de difundir la noticia de que Estonia había consolidado una cooperación internacional para localizar a los ciber criminales y ponerles ante la justicia, hizo que el número de atacantes disminuyera (54).

Después del ataque el gobierno estonio toma una serie de medidas políticas encaminadas a fortalecer la capacidad de prevención y respuesta ante incidentes informáticos, entre las cabe destacar: a) la firma de acuerdos de cooperación en incidentes informáticos con las principales entidades bancarias estonias, con los principales proveedores de servicio de internet y con las principales operadoras de telecomunicaciones; b) el impulso de iniciativas en el seno de la OTAN y de la Comisión Europea encaminadas a la cooperación con el sector privado; y c) el desarrollo y puesta en marcha de la Estrategia Nacional de Ciberdefensa

---

que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales.

(53) Op. Cit. 43 (3)

(54) Ibid

en la que identifica la infraestructura de información crítica y las acciones necesarias para su defensa.

Estonia dio al mundo tres lecciones de respuesta política a un ciber ataque masivo contra la seguridad nacional.

1. El gobierno identificó con celeridad que estaban bajo un ataque de gran dimensión que podía derivar en una crisis de seguridad nacional.
2. Formaron inmediatamente un equipo multifuncional para coordinar la respuesta; en el que se incluían expertos de la esfera técnica, política, militar, diplomática y jurídica.
3. Reconocieron desde el primer momento ante el mundo que estaban siendo víctimas de un ciber ataque (55).

Estas tres acciones fueron posibles debido a la formación y conocimiento que los políticos estonios tienen sobre el mundo de las tecnologías de la información; incluyendo el Presidente de la República de Estonia, Toomas Hendrik Ilves, que ha ejercido en diversos ocasiones de orador de apertura en conferencias internacionales relacionadas con el tema y demostrando un amplio conocimiento (56).

La respuesta legal

Toda respuesta legal ante este tipo de ciber ataques tiene dos caras, la nacional y la internacional. La nacional, con la aplicación de la legislación nacional aplicable a estos casos y la internacional, con la aplicación de los acuerdos bilaterales y multinacionales de cooperación en materia criminal.

Las autoridades estonias consideraron que los ciberataques debían ser tratados como crímenes cibernéticos y debían ser castigados de acuerdo con el código penal estonio y perseguidos e investigados de acuerdo con las leyes nacionales y los acuerdos internacionales.

Pero Estonia se encontró con dos problemas legales de difícil solución:

---

(55) No es práctica habitual por parte de ningún gobierno ni gran empresa reconocer que se ha sufrido un ciber ataque con éxito debido al miedo a la pérdida de fiabilidad y reputación.

(56) Ejemplos de sus discursos se pueden encontrar en la web oficial del presidente de la republica, www.president.ee. es digno de destacar su discurso de inauguración de la Conferencia sobre ciber conflictos, Tallinn 16-06-2010.

1.º Los legisladores estonios no previeron los ciberataques en la dimensión de lo acontecido en Estonia y la máxima pena prevista en el código penal, en la época del conflicto, para delitos de ataques cibernéticos era de un año. Esto hacía inviable la investigación en internet con el fin de identificar a los atacantes, pues la legislación estonia solo permitía la recolección y análisis de datos extraídos por medios electrónicos de internet relativos a personas individuales cuando el crimen que abre el proceso de investigación tiene asociado una pena de más de tres años (57).
2.º Cuando los atacantes, debido a la cooperación internacional, vieron que sus botnets estaban siendo anuladas movieron sus redes a jurisdicciones con menos o ninguna disposición o capacidad a cooperar, es decir movían sus elementos de ataque a «paraísos legales cibernéticos», como Egipto, Vietnam o Perú.

La cooperación internacional dio sus frutos en forma de alejar las botnets de sus territorios y de identificar potenciales direcciones IP fuente de los ataques, pero, por un lado, el desplazamiento de las botnets a paraísos ciber legales y por otro, el rechazo de países, como Rusia, a identificar, aprehender y poner a disposición judicial a las personas asociadas con las mencionadas direcciones IP hicieron infructuoso todo el trabajo legal acometido por las autoridades estonias (58).

El 10 de mayo de 2007, la oficina del fiscal general de Estonia, Norman Ass, tramitó un escrito oficial a su homólogo de la Federación Rusa, en base al acuerdo de ayuda legal mutua entre los dos países firmado en 1993, en la que se exhortaba a identificar a las personas que habían tomada parte en los ataques. En el escrito se incluía información detallada de direcciones IP, sitios web y foros de internet localizados en territorio de la Federación Rusa que estaban involucrados en los ataques.

Una de las direcciones IP implicadas pertenecía al gobierno de la Federación Rusa (59) y fuentes oficiales estonias declaraban que en la

(57) Op. Cit. 31. // Paradójico, la democracia y las libertades públicas impidieron la persecución de delitos que atentaban contra la propia democracia y las libertades públicas.
(58) Es claro desde un punto de vista legal, que solo las personas individuales y no las direcciones IP pueden ser puestas a disposición judicial.
(59) Gadi Evron, en su artículo «Battling botnets and online mobs» en la revista «Science & Technology» Winter/spring 2008, página 125.

investigación forense habían identificado direcciones IP que pertenecían a la administración presidencial y agencias estatales rusas (60).

Un año y un mes más tarde de la petición, Estonia recibe la respuesta en la que Rusia rechazaba la cooperación alegando que lo requerido no estaba contemplado en el acuerdo de ayuda legal mutua del 93.

La falta de cooperación de Rusia era tan manifiesta que incluso Rein Lang, Ministro de Justicia estonio llego a declarar sobre las autoridades rusas: «ni siquiera descuelgan el teléfono» (61).

A día de hoy sólo una persona relacionada con el conflicto, Dmitri Galushkevich (62), ha podido ser declarado culpable. Su delito, «bloqueo ilegal de datos informáticos con el propósito de obstaculizar el funcionamiento de un sistema informático»; la condena, el pago de una multa de 22.900 coronas estonias (1.464 Euros).

En definitiva, el caso Estonia lanza un mensaje al mundo: «cometer ataques cibernéticos puede salir gratis o, en todo caso, muy barato».

Investigación forense

Una vez que se recupera la normalidad en la vida de los estonios, es momento de hacer análisis y valoración de los hechos.

La investigación forense se basa en la recolección y estudio de toda la actividad cibernética registrada (63) y rastrea la ruta de los ataques en sentido inverso hasta llegar a la fuente o centro de mando y control de la botnet.

Para acceder hasta el origen es necesario el permiso y la cooperación de las autoridades de los territorios por donde el ataque transcurrió, y como ya se ha mencionado previamente, en el caso de la Federación Rusa, el permiso no fue obtenido.

A partir de este hecho se abren todo tipo de especulaciones e hipótesis, ya que, las direcciones IP asociadas a organismos estatales y gubernamentales rusos, podían ser los orígenes de los ataques o podían

(60) Op. Cit. 29
(61) Ibid
(62) Dmitri Galushkevich, ciudadano estonio de etnia rusa, en el momento del ciber conflicto tenía 19 años de edad y estudiaba en la Universidad de Tecnología de Tallinn.
(63) Mediante el análisis de logs.

ser direcciones IP asociadas a máquinas secuestradas que formaban parte de la ruta o itinerario del ataque, pero no el origen.

Diferentes datos ilustran sobre la magnitud del evento: más de 178 países estuvieron involucrados (64); 128 ataques DDoS en dos semanas, de los cuales, 58 fueron en un solo día; y algunos ataques llegaron hasta los 200 Mbps(65).

Conclusiones

– La implicación de Rusia y de ciudadanos rusos en los ataques no ofrece ninguna duda a la luz del número de evidencias recolectadas: el tráfico malicioso a menudo contenía elementos de motivación política en lengua rusa, instrucciones precisas de cuándo, cómo y qué atacar fueron diseminadas por números foros, blogs y sitios web rusos (66).
  Según Ene Ergma, los ciberataques fueron un test para comprobar la capacidad de respuesta y el nivel de organización de la OTAN (67). Según Rain Ottis, fueron una operación de información rusa contra Estonia (68).
  Pero sin duda los datos más consistentes de la implicación de las autoridades rusas en el asunto, si bien no claramente como autores materiales pero sí como inductores, colaboradores necesarios o cómplices, son: a) la renuncia por parte del gobierno ruso a acatar el acuerdo de ayuda legal mutua con Estonia, b) la dejación de funciones por parte de las autoridades rusas en el bloqueo durante dos semanas de la embajada estonia en Moscú o en la agresión a la embajadora y c) la presión económica ejercida por Rusia coincidiendo con los ciberataques, evidenciada por el corte de la frontera a transportes pesados procedentes de Estonia, cancelaciones de contratos de importación de productos fabricados en Estonia, cancelación de transportes ferroviarios, como el que unía San Petersburgo con Tallín, etc. (69).

(64) Según Katrin Parmage, portavoz del Centro Informático Estatal de Estonia en un artículo de Marge Tubalkain-Trell para el Baltic Bussiness News, http://balticbusinessnews.com/?PublicationId=b737410e-e519-4a36-885f-85b183cc3478
(65) Op. Cit. 31
(66) Op. Cit. 14
(67) Op. Cit 48
(68) Op. Cit 11
(69) Op. Cit 14

– La amenaza cibernética es real y muy atractiva para los que quieran causar un gran daño corriendo mínimos riesgos.
– La amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede afectar a la infraestructura crítica nacional conllevando riesgos de daños físicos para la población.
  Un ejemplo claro de esto es el «gusano Stuxnet», un código malicioso que, según los investigadores, es capaz de tomar el control de los sistemas de control automatizados de las fábricas que previamente ha infectado y puede llevar a cabo acciones para las que está programado.
  A través de la ingeniería inversa del código del Stuxnet, expertos en ciber seguridad de los Estados Unidos declaran que el «Stuxnet es esencialmente un misil cibernético de precisión de carácter militar, desarrollado a principios de 2009 y diseñado para destruir un objetivo de alta importancia del mundo real, como una planta nuclear».
– El derecho a disponer de ciber armamento, es un derecho de toda sociedad democrática para poder hacer frente, con los mismos medios, a aquellos que quieren perjudicar sus legítimos intereses.

Otro ciber caso interesante, por ser el primer caso en el que se combinan operaciones militares y operaciones cibernéticas, es el Caso Georgia 2008. Como en el caso Estonia, hay hechos suficientes que inducen a pensar que el gobierno de la Federación Rusa estuvo detrás de la coordinación de las ciber operaciones, pero, a día de hoy, la demostración legal no es posible.

EL CIBER CASO GEORGIA 2008

Presumiblemente, y acorde con el análisis lógico de los hechos acontecidos, Rusia acumuló experiencia en la desestabilización de países a través de las ciber operaciones contra Estonia en 2007 y contra Lituania en 2008. ¿Por qué no dar un paso más y combinar las operaciones armadas con las cibernéticas?

Después de su experiencia con Estonia y Lituania, la primera oportunidad que se le presenta para practicar su capacidad conjunta «Fuerzas Armadas - Fuerzas Cibernéticas» es en el conflicto con Georgia. Vayamos al asunto.

Antecedentes

Georgia es un país que limita al norte con Rusia, al este con Azerbaiyán, al sur con Armenia y Turquía y al oeste con el Mar Negro. Tiene una población de 4.601.000 habitantes y una superficie total de 69.500 km². Es un país poco desarrollado en materia de tecnología de la información, lo que hace que el desarrollo de sus actividades políticas, sociales y financieras sean poco dependiente de las TI y por consecuencia los ciber ataques causan un menor daño que en el caso Estonia; pero por otro lado, esa falta de desarrollo tecnológico hace que su capacidad de respuesta ante ciber ataques sea también reducida.

Osetia del Sur es un territorio situado en el Cáucaso en la frontera entre la Federación Rusa y Georgia. Tiene una población aproximada de 80.000 habitantes y una superficie total de 3.900 km². Durante la época soviética tenía la consideración de Óblast (70) Autónomo dentro de la República Socialista Soviética de Georgia.

En 1989 la región de Osetia del Sur declaró unilateralmente su independencia tras vencer en una guerra con Georgia y se convirtió en una república independiente de facto, pero Georgia –y la mayor parte de la Comunidad Internacional (71)–, siempre la ha considerado como parte de su territorio, como así lo era en la época soviética.

Debido a esta disparidad de criterios la región era un foco continuo de conflictos. Para tratar de lograr y mantener la estabilidad en la zona, en 1992 se creó una fuerza de mantenimiento de la paz bajo mandato de la OSCE (72). La fuerza de mantenimiento de la paz estaba compuesta por tropas de Rusia, Georgia y Osetia del Sur y el mando lo ostentaba la Autoridad Militar Rusa (73).

El 7 de agosto de 2008 se inició la Guerra de Osetia del Sur entre Georgia, por un lado, y Osetia del Sur, Abjasia y Rusia por el otro; con una ataque, que por sorpresa, realizaron las Fuerzas Armadas de Georgia contra Fuerzas Separatistas.

---

(70) Óblast: En la extinta Unión de Repúblicas Socialistas Soviéticas, los óblasts eran entidades administrativas de tercer nivel, el primer nivel era la propia URSS, el segundo nivel era la República que a su vez se componía de Óblasts.

(71) A día de hoy, solo Rusia, Abjasia, Nauru, Nicaragua y Venezuela reconocen oficialmente a Osetia del Sur como Republica Independiente.

(72) OSCE: Organización para la Seguridad y la Cooperación en Europa.

(73) Algo así como «poner al lobo a cuidar del rebaño».

Este hecho provocó la reacción inmediata de Rusia, que consideró el hecho un ultraje contra ciudadanos rusos fuera de las fronteras y consideró su obligación defenderles de tal ultraje.

Al día siguiente, el 8 de agosto de 2008, los rusos iniciaron una serie de operaciones militares en territorio de Osetia del Sur, extendiéndose posteriormente a otras regiones de Georgia y al Mar Negro; más allá de la zona de responsabilidad del mandato OSCE de mantenimiento de la paz.

El 9 de agosto de 2008, el presidente de Georgia, Mikheil Saakashvili, declaró el estado de guerra, al considerar los hechos acontecidos como una agresión Militar por parte de la Federación Rusa contra Georgia.

Tres días más tarde, el 12 de agosto de 2008, el Presidente de la Federación Rusa, Dmitri Medvédev, decreta el fin de las operaciones militares rusas en territorio georgiano y acepta el plan de paz propuesto por la Unión Europea; plan que entre otras cosas obliga a las Fuerzas a volver a las posiciones anteriores al comienzo del conflicto.

Cronología de los ciber ataques

Los ciber ataques contra Georgia se produjeron en tres fases diferenciadas:

– 1.ª fase: Pre-conflicto armado. Junio de 2008-7 de agosto de 2008. Ataques de pequeña escala.

Durante este periodo se contabilizaron ataques DDoS de pequeña escala contra sitios web oficiales de Georgia. El primer ciber ataque fue registrado en Junio de 2008, dos meses antes del inicio del conflicto (74). Estos ataques se enmarcan dentro de las tensas relaciones que mantenían Rusia y Georgia

– 2.ª fase: Conflicto armado. 8 de agosto de 2008 – 12 de agosto de 2008. Ataques bien organizados y coordinados.

Durante los cinco días que duró el conflicto armado se sucedieron ciber ataques contra sitios web pertenecientes al Presidente de la República de Georgia, el Parlamento, Ministerios de Defensa y Asuntos Exteriores, el Banco Nacional y las principales agencias de noticias.

(74) Artículo publicado en el «Washington Post» por Kim Hart, el 14 de agosto de 2008, «Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar». http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623_pf.html

El primer ataque a gran escala y con un alto grado de sofisticación en su ejecución se produjo coincidiendo con la primera ofensiva de las Fuerzas Rusas en territorio de Georgia.

Es importante destacar, que a medida que el conflicto armado se intensificaba, a su vez se incrementaba el número de ciber ataques (75).

Deliberadamente o no, el caso es que, los ciber ataques debilitaron la capacidad de toma de decisiones del entorno político y militar de Georgia durante el conflicto; y debilitaron la capacidad de información y de comunicación entre el Gobierno y los ciudadanos, a la vez que, a través de la ciber propaganda, trataron de influenciar en la opinión pública hacia la postura defendida por Rusia, Osetia del Sur y Abjasia.

– 3ª fase: Post-conflicto armado. 13 de agosto de 2008 – 28 de agosto de 2008. Ataques de menor escala.

Coincidiendo con la finalización del conflicto armado, el 12 de agosto de 2008, las operaciones cibernéticas sufrieron una importante reducción en número e intensidad pero el conflicto en el ciber espacio, parecía no estar incluido en el acuerdo de paz y las ciber operaciones continuaron hasta el 28 de agosto.

El fin de las operaciones cibernéticas no se debió a ningún tipo de acuerdo, sino a la falta de rentabilidad de los ciber taques. Por un lado las medidas de ciber defensa lograron bloquear gran parte de los ciber ataques y por otro, el entusiasmo de los hacktivistas iba decreciendo después de la finalización del conflicto armado.

El último gran ataque contra Georgia fue registrado el 27 de agosto de 2008.

Tipos de ataques

Los tipos de ataques fueron parecidos al caso Estonia de 2007, no especialmente sofisticados pero si muy efectivos y tuvieron influencia en el desarrollo de las operaciones armadas.

(75) Roland Heickero, Swedish Defence Research Agency, en la publicación «Emerging Cyber Threats and Russian Views on Information Operations». http://www2.foi.se/rapp/foir2970.pdf

Los tipos de ataques llevados a cabo en el caso Georgia fueron principalmente (76):

a) Ataques prolongados y múltiples de tipo «ICMP flood», «TCP SYN flood», «HTTP flood» contra web sites oficiales;
b) Ataques DDoS a través de botnets, con centros de mando y control dispersos en diferentes países, que hacían uso de «scripts» (77) no especialmente sofisticados, mejor organizados –técnica y operativamente–, mejor coordinados, con mayor poder dañino y con un mayor número de participantes que en el caso Estonia, y
c) Ataques de tipo inyección SQL, no especialmente sofisticados pero bien planeados y organizados y que se basaban en reconocimientos de objetivos y evolución continua de los ataques acorde con la inteligencia obtenida. Estos ataques son de difícil detección.

Las redes sociales fueron ampliamente utilizadas como instrumento para reclutar voluntarios y para la descarga de «malware».

Objetivos

La elección de los objetivos perseguía la finalidad de causar una pérdida de capacidad operativa y de confianza en las instituciones políticas, militares y financieras del país y bloquear la capacidad de comunicación entre dichas instituciones, entre el gobierno estonio y sus ciudadanos y entre Georgia y el mundo exterior.

Los objetivos políticos se concretaron en los sitios web del Presidente de la República de Georgia, del Parlamento, del Ministerio de Asuntos Exteriores, del Ministerio de Ciencia y Educación, de Instituciones Educativas (78).

Los objetivos militares se concretaron en los sitios web del Ministerio de Defensa (79).

Los objetivos financieros se concretaron en los sitios web del Banco Nacional de la República de Georgia y de la mayor institución bancaria del país (TBC) (80).

---

(76) José Nazario (Arbor Network) y Andre M. DiMino (Shadowserver Foundation), en la publicación «An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008».
(77) Un script es un programa simple de ordenador, desarrollado para realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario.
(78) www.president.gov.ge, www.parliament.ge, www.mfa.gov.ge, www.mes.gov.ge, www.naec.gov.ee
(79) www.mod.gov.ee
(80) www.nbg.gov.ge, www.tbc.ge

Y los objetivos de comunicaciones se concretaron en los sitios web y foros de las principales agencia de comunicaciones, agencias de noticias y televisión (81).

La respuesta técnica

Georgia disponía de reducida capacidad técnica para hacer frente a los ciber ataques, por lo que la cooperación internacional, tanto institucional como privada fue fundamental para hacer frente a los ataques.

La respuesta técnica en el caso de Georgia fue principalmente el bloqueo del dominio «.ru» y el traslado de los sitios web a otras plataformas fuera de las fronteras georgianas.

La respuesta política

Georgia tuvo gran facilidad para acceder al apoyo multinacional debido a los precedentes de Estonia y Lituania, fundamentalmente.

Estonia contribuyó, de inmediato, enviando expertos del CERT-EE para ayudar en la respuesta técnica. La contribución de estos expertos fue fundamental debido a la experiencia adquirida un año antes. Además, ofreció su infraestructura para alojar sitios web oficiales de Georgia.

Polonia también fue rápida en su apoyo, prestando su infraestructura para alojar sitios web que habían quedado fuera de servicio.

Entre la cooperación privada es de destacar la de las empresas americanas Google y Tulip Systems Inc., cuyo director ejecutivo es un expatriado georgiano, Nino Doijashvili. Ambas, entre otras cosas, cedieron su infraestructura para hospedar las webs atacadas.

La respuesta legal

Como se puede suponer, Georgia encontró las mismas dificultades para forzar una respuesta jurídica en este asunto, puesto que el presunto origen de los ciberataques se sitúa en territorio ruso, y la cooperación para identificar a los responsables no es aceptada por quién tiene facultad para ello.

---

(81) www.forum.ge, www.civil.ge, www.presa.ge, www.aspny.ge, www.rustavi2.com, www.news.ge, www.interpress.ge, www.tblisiweb.info, www.os-inform.com, www.hacking.ge

Pero además en este caso se da la circunstancia de la coincidencia de un conflicto armado y un conflicto cibernético que invita a pensar en la aplicación de la ley de conflictos armados –LOAC–, que se aplica a los conflictos armados internacionales y en la conducción de operaciones militares y de «actividades relacionadas con los conflictos armados».

Investigación forense

El proyecto Grey Goose 2 (82), identificó dos sitios web rusos desde donde se organizaron cibera taques coincidiendo con el conflicto armado: «www.stopgeorgia.ru» y «www.xakep.ru».

En estos sitios se informaba detalladamente de los pasos a seguir para atacar sitios georgianos; se detallaban listas de objetivos, se ofrecían descargas de programas ad hoc para participar inmediatamente en ataques masivos DDoS, se animaba a la participación a simpatizantes con la postura rusa y toda la información era actualizada permanentemente.

La web «stopgeorgia.ru» fue creada poco tiempo después –en pocas horas– de que las Fuerzas Rusas invadieran el territorio de Osetia del Sur; usaba una dirección IP relacionada con el proveedor de servicios Steadyhost –www.steadyhost.ru– que tiene su registro en Nueva York pero que es operado desde San Petersburgo. Se piensa que este proveedor tiene sus oficinas en el mismo edificio que el Centro de Investigación de la Capacidad Militar de Países Extranjeros del Ministerio Ruso de Defensa.

De las investigaciones realizadas por las diferentes instituciones y expertos que siguen ciber incidentes por todo el mundo, como la Fundación Shadowserver o Arbor Networks; se deducen los siguientes datos: a) Los ciber ataques fueron de mayor intensidad que los registrados en el caso Estonia 2007, b) el 90 % de los ataques fueron llevados a cabo por voluntarios o hacktivistas (83) y c) sitios web oficiales de Georgia –incluidos entidades bancarias– estuvieron fuera de servicio durante días.

(82) El proyecto Gery Goose 2 es una iniciativa de Inteligencia de Fuentes Abiertas (Open Source Intelligence -OSINT) lanzada el 22 de agosto 2008 y cuya misión era examinar cómo se desarrollaron las operaciones cibernéticas Rusas contra Georgia y analizar los responsables, en concreto analizar la implicación del gobierno ruso y de los movimientos de voluntarios rusos patrióticos.

(83) Shaun Waterman, «Analysis: Russia-Georgia cyberwar doubted». http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyberwar_doubted_999.html

Conclusiones

a) Como en el caso Estonia, la participación del gobierno ruso no ha sido probada hasta la fecha; aunque existen suficientes indicios para deducir que Rusia es, al menos, cómplice en la organización de los ciber ataques. Los indicios están fundamentalmente basados en tres hechos: a) la falta de cooperación de Rusia para identificar a los responsables; b) Rusia es el principal o único beneficiario de los resultados de la ofensiva cibernética y c) los ciber ataques evolucionaban acorde con la evolución de las operaciones armadas y para ello se necesitaba información que solo era accesible por parte de las autoridades políticas y militares rusas.
b) Las ciber operaciones estuvieron bien planificadas, organizadas y coordinadas en tiempo y espacio; existían webs donde se emplazaba información detallada para unirse a los ataques y programas ad-hoc para realizar ciber ataques que producían resultados beneficiosos para Rusia en el conflicto armado con Georgia y además, dichos ciber ataques evolucionaban de acuerdo con la inteligencia obtenida. Esto no solo requiere el uso de operaciones cibernéticas ofensivas (CNA (84)) sino de operaciones cibernéticas de explotación (CNE (85)).
c) Las ciber operaciones fueron iniciadas y conducidas en conjunción con las operaciones armadas y sirvieron para debilitar la capacidad de respuesta militar y política de Georgia, como operaciones psicológicas y desmoralizantes al bloquear la comunicación entre el Gobierno y el pueblo georgiano y como operaciones propagandísticas para reclutar adeptos a la causa Rusa.
d) El uso de patriotas voluntarios es una herramienta al alcance de los gobiernos para realizar operaciones cibernéticas (CNO) contra otros países y evitar la imputación legal.

LA CIBERSEGURIDAD EN LA OTAN

El ciber ataque de la primavera de 2007 a Estonia representa un hito y un reto histórico para la OTAN; es la primera vez que un estado miem-

(84) Las operaciones cibernéticas o CNO (Computer Network Operations) se componen de operaciones de ataque (CNA, Computer Network Attack); operaciones de defensa (CND, Computer Network Defence) y de operaciones de explotación (CNE, Computer Network Exploitation).
(85) Ibid.

bro solicita apoyo a la OTAN por un ataque a la infraestructura crítica de información del país.

Se da la paradójica situación de que la mayoría de los expertos en ciber seguridad de la OTAN se enteran de la noticia en Washington, mientras atendían al congreso de ciber seguridad (86) que anualmente organiza la Oficina de Seguridad de la Alianza (87).

Como queda demostrado por los hechos, la OTAN no disponía de una plan de acción en caso de ciber ataque a un estado miembro; hasta ahora se habían considerado problemas de índole nacional, puesto que muchas naciones de la OTAN y en especial los Estados Unidos de América recibían y reciben a diario ciber ataques –de la misma envergadura y mayor– contra la infraestructura crítica de información del país, sin que esto constituya causa de intervención por parte de la OTAN.

Pero el caso de Estonia es diferente, pues debido a la dimensión del país (88), los ataques le llevaron una situación de crisis de seguridad nacional. La intervención de la OTAN, de alguna manera, era más que justificada. Pero no había un plan de acción.

No solo los ciberataques a Estonia representaron un caso de reflexión para la OTAN, también otros casos, como el ciberataque a Lituania (89) en julio de 2008, el ciber ataque a Georgia en julio de 2008 y el ciber ataque a Kirguistán en enero de 2009 (90).

La OTAN se enfrentó con el problema de manera decidida en la cumbre de Bucarest (91), celebrada entre los días 2 y 4 de abril de 2008. Como consecuencia de la reunión se llegó al acuerdo expresado en la sección 47 de la declaración de la cumbre:

> *«La OTAN se mantiene comprometida con el fortalecimiento de los sistemas de información crítica de la Alianza contra ciber ataques. Hemos adoptados recientemente la Política de Ciber Defensa, y estamos desarrollando las estructuras y autoridades para llevarla*

(86) NATO Cyber Defence Workshop 2007, Washington, Estados Unidos
(87) NOS: NATO Office of Security
(88) Op. Cit. 34
(89) Lituania es un país miembro de la OTAN desde el 24 de marzo de 2004.
(90) Georgia y Kirguiztán son dos naciones con una estrecha relación de cooperación con OTAN a través de su participación en el partenariado por la paz (Partner for Peace) desde 1994.
(91) http://www.summitbucharest.ro/en/1.html

a cabo. Nuestra política en materia de Ciber Defensa subraya la necesidad de la OTAN y de las naciones miembros de proteger los sistemas de información crítica conforme con sus respectivas responsabilidades; compartir las mejores prácticas y establecer una capacidad de apoyo a las naciones, bajo petición, para contrarrestar un ciber ataque. Continuamos con el desarrollo de las capacidades de ciberdefensa de la OTAN y con el fortalecimiento de los vínculos entre la OTAN y las autoridades nacionales».

De la declaración se desprenden tres líneas de acción principales: a) medidas a adoptar por la propia OTAN para mejorar su capacidad de ciber defensa, b) medidas a adoptar por las naciones para mejorar la protección de los sistemas de información crítica desplegados en sus territorios y c) medidas a adoptar por ambas partes, OTAN y Naciones, para mejorar la coordinación, el intercambio de información y el apoyo mutuo.

En este capítulo, se tratará de la acción a) medidas adoptadas por la OTAN para mejorar su capacidad de ciberdefensa; dejando las siguientes acciones para otros capítulos de este cuaderno.

La Ciberdefensa en la OTAN

La OTAN a posteriori de los ciberataques a Estonia, realiza un análisis y estudio del caso y elabora un informe de lecciones aprendidas (92).

Como consecuencia del estudio, se concluye que la OTAN no sólo no disponía de un plan de acción en caso de ciber ataque, sino que ni siquiera disponía del concepto de Ciberdefensa y su correspondiente política.

El 7 de enero de 2008, es una fecha clave para la Ciberdefensa en la OTAN; el Consejo firma la Política de Ciber Defensa de la OTAN (93) con el objetivo de mejorar la capacidad de la OTAN para proteger los sistemas de información y comunicaciones (CIS) de importancia crítica para la Alianza contra ciber ataques.

(92) «Report of the examination of the lessons learned from the recent cyber attacks», AC/322-D(2007)0050 -01.10.2007.
(93) «NATO Policy on Cyber Defence», C-M(2007)0120.

Como consecuencia de la política, la OTAN impulsa una serie de acciones para mejorar su capacidad de ciberdefensa, entre las que se destacan:

a) Desarrollo del concepto (94) de Ciberdefensa (95).
b) Impulso y apoyo para adquirir cuanto antes la capacidad operativa completa de respuesta ante incidentes informáticos (96).
   La OTAN disponía de una hoja de ruta para lograr la capacidad operativa completa de respuesta ante incidentes informáticos (NCIRC FOC)(97). El caso Estonia tuvo un efecto catalizador para acelerar el proceso; en el momento de los ataques la OTAN disponía de una capacidad inicial (NCIRC IOC) (98).
   La NCIRC consta de un centro de apoyo y coordinación de ciberdefensa (CDCSC(99)) y de un centro técnico (NCIRC TC)(100), lo que se puede considerar el NATO CERT. En estos dos centros se concentran gran parte de los expertos de seguridad de la OTAN.
   Debido a que la respuesta ante un ciber ataque es multidisciplinar, este centro coordina su trabajo con otras entidades –consejos, grupos de trabajo, agencias, centros, etc– con responsabilidad en diversas materias dentro de la OTAN, como política de la alianza, estandarización, recursos, relaciones públicas, asuntos jurídicos, asuntos económicos, acreditación de sistemas de seguridad, inteligencia, coordinación con países miembros, comunicaciones y otras áreas de seguridad como seguridad del personal, de las instalaciones, de la documentación, etc.
c) Impulso y apoyo para establecer cuanto antes el Centro de Excelencia de Ciber Defensa Cooperativa de la OTAN (CCDCOE) (101).
   El 28 de octubre de 2008 se establece oficialmente en Tallinn, capital de la República de Estonia, el Centro de Excelencia de la OTAN de Ciberdefensa Cooperativa; con la misión de mejorar la

(94) NATO Cyber Defence Concept, MC 0571, 04.02.2008
(95) No se puede profundizar mucho en el tema debido a que la mayoría de la información disponible es clasificada.
(96) Ibid.
(97) NCIRC FOC: NATO Computer Incidents Response Capability Full Operational Capability.
(98) NCIRC IOC: NATO Computer Incidents Response Initial Full Operational Capability.
(99) CDCSC: Cyber Defense Coordination and Support Centre.
(100) NCIRC TC: NATO Computer Incidents Response Capability Technical Centre.
(101) CCDCOE: Cooperative Cyber Defence Centre of Excellence (CCDCOE) Para más información: www.ccdcoe.org

capacidad y cooperación de la OTAN y sus estados miembros en Ciberdefensa a través del desarrollo de programas y proyectos de I+D+I, de formación, de análisis de casos reales y de consulta.
El centro está formado, a día de la publicación de este cuaderno, por personal experto en ciber seguridad procedente de 10 países: Estonia como país anfitrión, Alemania, EEUU, Eslovaquia, Hungría, Italia, Letonia, Lituania, Turquía y España.
La visión del Centro es dar respuestas y soluciones globales a problemas concretos y para ello los proyectos son acometidos por equipos multidisciplinares, en los que se involucran personal experto en ciber seguridad y especializado en tres ramas fundamentalmente: asuntos operativos, funcionales y militares; asuntos tecnológicos, académicos y científicos; y asuntos legales.
El centro depende jerárquicamente de un Comité de Dirección compuesto por representantes de los países componentes (102) y de la OTAN y tiene el estatus legal de Organización Militar Internacional. Dicho estatus le confiere al CCDCOE relación ambivalente con la OTAN; por un lado no forma parte de la estructura de mando la OTAN y por lo tanto no recibe ningún tipo de financiación por parte de la Alianza, y como consecuencia goza de cierta independencia; y por otro lado, está obligado a considerar las peticiones de la OTAN con la más alta prioridad.
Esta ambivalencia le confiere al centro unas características particulares en beneficio de los resultados de los proyectos que acomete: de facto está incluido en la estructura organizativa de ciberdefensa de la OTAN, formando parte del consejo de gestión de Ciber Defensa (NATO CDMB (103), se comenta en el siguiente apartado), mantiene una relación directa y estrecha con ambas partes de la ciberdefensa de la OTAN, la ciberdefensa operativa (NCIRC) y la ciberdefensa estratégica (NATO ACT) (104); pero por otro lado, mantiene una actividad significativa de colaboración con el sector privado y el sector académico y universitario.

d) La creación de la Autoridad para la gestión de la Ciber Defensa (NATO CDMA (105)) (106).

(102) El representante nacional español en el comité de dirección del CCDCOE es el jefe de la sección INFOSEC del Estado Mayor de la Defensa.
(103) CDMB: Cyber Defence Management Board.
(104) NATO ACT: NATO Allied Command of Transformation.
(105) CDMA: Cyber Defence Management Authority.
(106) Op. Cit. 98

La creación de la Autoridad para la gestión de la Ciber Defensa, es quizás el hito más importante en el proceso de construcción de la ciber seguridad de la OTAN. Es el establecimiento de una única autoridad con responsabilidad y medios para coordinar todas las actividades de ciberdefensa y las respuestas ante ciber incidentes. Es como dice el investigador Rex B. Hughes: «al contrario de como sucedió durante el ataque a Estonia, las naciones de la OTAN ahora disponen de un número de teléfono al que llamar en caso de una emergencia cibernética (107)»

La CDMA coordina todos los asuntos de Ciberdefensa a través del consejo de gestión de Ciberdefensa (CDMB) del que forman parte representantes de todas las autoridades de la OTAN, incluyendo el Consejo del Atlántico Norte (NAC); el comité militar (MC), las autoridades de emergencia política y civil, la autoridad de gestión de la política (NPMA (108)) y el comité de seguridad (NSC (109)); y es supervisado por el consejo de gestión de consulta, mando y control (NC3B (110)).

La misión de la CDMA es revisar y coordinar las capacidades de Ciberdefensa de la OTAN, centrándose particularmente en: a) la amenaza cibernética, b) en la gestión del riesgo de seguridad, c) en la valoración de las vulnerabilidades y d) en la continuidad de negocio de los sistemas de información y comunicaciones críticos para el funcionamiento de la alianza.

La cuestión es que la capacidad orgánica de Ciberdefensa de la OTAN no es suficiente para parar y disuadir ciber ataques; los ataques a la OTAN pueden ser dirigidos y redirigidos desde fuera del territorio responsabilidad de la OTAN (especificado en el artículo 6 (111) del tratado de Washington, por lo que es necesario que la

(107) El Doctor Rex B. Hughes es cofundador y director del proyecto de Ciberseguridad en Chatham House, Londres y es un investigador asociado de la Universidad de Cambridge-Instituto MIT. Actualmente sus investigaciones se centran en el análisis de cómo la ausencia de un marco coherente de seguridad cibernética a nivel mundial puede amenazar la integridad estructural del orden comercial internacional.

(108) NPMA: NATO Policy Management Authority.

(109) NSC: NATO Security Committee.

(110) NC3B: NATO Consultation, Command and Control.

(111) Tratado de Washington, Art. 6: A efectos del artículo 5, se considerará ataque armado contra una o varias de las Partes, el que se produzca: a) Contra el territorio de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer. b) Contra las fuerzas, buques o aeronaves de cualquiera de las

OTAN trabaje y consolide alianzas con países y organizaciones que no forman parte de la OTAN.

e) La creación de la Autoridad Militar para la gestión de la Ciber Defensa con la misión de revisar y coordinar las capacidades militares de Ciberdefensa de la OTAN (112).

La amenaza cibernética y el artículo 4 del tratado de Washington

El artículo 4 del tratado de Washington dice:

«Las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada.»

¿Qué indicadores reflejarían de manera objetiva que un ciber ataque determinado atente contra *la integridad territorial, la independencia política o la seguridad* de un país miembro de la OTAN?

El art. 4 trata exclusivamente del derecho de consulta y a juicio de una sola de las partes, con lo que se entiende que no es necesario que se dé una situación objetiva y de consenso entre todas las partes para ejercer el derecho.

No obstante, debido a las peculiaridades del ciber espacio, no estaría de más que las naciones y la OTAN, estudiaran y redefinieran el concepto de «integridad territorial» y «seguridad». Actualmente el concepto de integridad territorial(113) se ha considerado basado en la defensa de las fronteras físicas de un país. ¿Es este concepto aplicable al ciber espacio?

La amenaza cibernética y el artículo 5 del tratado de Washington

El artículo 5 del tratado de Washington dice:

«Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, sea con-

---

Partes que se hallen en estos territorios, como en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer.

(112) Op. Cit 98

(113) La integridad territorial es un principio del derecho internacional que evoca el derecho y deber inalienable de un Estado de preservar sus fronteras de toda influencia exterior. Implica, por lo tanto, que los Estados no deben promover movimientos secesionistas o cambios en las fronteras de otros, cambios que se consideran actos de agresión.

siderado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudar a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales.»

Consideraciones al respecto:

1. ¿Qué es un ataque armado?, ¿Se puede considerar un ciber ataque un ataque armado?

   Un ataque armado se puede considerar todo ataque que haga uso de un arma. Y según la Real Academia Española un arma es entre otras acepciones:

   1. *f. Instrumento, medio o máquina destinados a atacar o a defenderse.*

   2. *f. Mil. Cada uno de los institutos combatientes de una fuerza militar. El arma de infantería, de caballería, de artillería*

   4. *f. pl. Conjunto de las armas que lleva un guerrero o una unidad de guerra.*

   Y considera, entre otras, los siguientes diferentes tipos de armas: arma acorazada, aérea, antiaérea, arrojadiza, atómica, automática, blanca, defensiva, de fuego, de mano, de percusión, de precisión, mecanizada, motorizada, naval, nuclear, ofensiva, pesada, semiautomática.

   De acuerdo con la acepción 4. de la RAE, arma es el *conjunto de las armas que lleva un guerrero o una unidad de guerra.* Según esta acepción el conjunto de armas de un ciber guerrero o una ciber unidad estaría basado en hardware y software.

   De acuerdo con la acepción 2. de la RAE, arma es un c*ada uno de los institutos combatientes de una fuerza militar. El arma de infantería, de caballería, de artillería*. Aunque, oficialmente, pocos países consideren el arma o la fuerza cibernética dentro de su estructura de mando militar; de facto es que la mayoría de los países

avanzados gozan de unas fuerzas militares específicas, entrenadas y equipadas para la ciberdefensa (114). La Ciber Fuerza es una realidad.

La acepción que es realmente relevante para el caso que nos ocupa es la primera, arma es un *instrumento, medio o máquina destinados a atacar o a defenderse*.

Según esta definición, no cabe duda de que un código malicioso –software– diseñado para atacar un sistema de información, un sistema de control industrial o una infraestructura crítica, es un arma y por consiguiente un ciber ataque es en toda regla un ataque armado.

En algunos foros se discute que para ser considerado un ataque armado debe haber destrucción física de por medio. Pero a día de hoy nadie discute que existe tecnología suficiente para diseñar códigos que causen destrucción y daños físicos (115).

El artículo 51 de la Carta de las Naciones Unidas reconoce el derecho de legítima defensa al afirmar que «Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de *ataque armado* contra un Miembro de las Naciones Unidas». Con lo cual, la ONU no da más luz al asunto pues abunda en el mismo término, ataque armado.

De acuerdo con lo expresado, el autor considera que un ciber ataque es un ataque armado que puede dar lugar a la invocación del artículo 5 por parte de la nación OTAN víctima.

Otra cosa es, dilucidar en qué situaciones el ciber ataque es lo suficientemente grave como para invocar el artículo 5.

2. ¿Dónde poner el límite de aplicación del art. 5?

   Ardua tarea dilucidar que parámetros pueden ayudar a tomar la decisión de aplicar o no el artículo 5.

   Considerar el volumen o fuerza de los ataques no es muy relevante, pues lo que para países de dimensiones reducidas es una situación de crisis nacional, para otros, como los Estados Unidos, es el pan de cada día. Según José Nazario, el tamaño (100-200 Mbps) de los ataques sufridos por Estonia no es realmente novedoso, es un tipo de ataque de tamaño común (116).

---

(114) Más información en el cuaderno de la cátedra ISDEFE-UPM, «Seguridad Nacional y Ciberdefensa». Ver bibliografía.

(115) En el artículo de F-Secure en http://www.f-secure.com/weblog/archives/00002040.html, se describe minuciosamente cómo un código software malicioso puede causar, entre otras cosas, que una fábrica explosione.

(116) Op. Cit. 24

Además los Estados o grupos beligerantes pueden evitar la aplicación del artículo 5 mediante la utilización de las tácticas de guerra de baja intensidad (117) (118).

Considerar la integridad territorial, la independencia política o la seguridad nacional como criterios es controvertido debido a la falta de objetividad y a la falta de definición de los conceptos en el ciber espacio.

Hoy por hoy la única manera de dilucidar el asunto es caso por caso, pero eso llevaría un tiempo de estudio que podría ser demasiado largo en un tipo de guerra donde la respuesta tiene que ser inmediata.

En definitiva se necesitan planes de acción y equipos de reacción rápida para casos de ciber ataques, independientemente del proceso de toma de decisión de la aplicación del artículo 5; y la OTAN está trabajando en ello.

3. ¿Contra quién se aplicaría el art.5?

   Uno de los grandes problemas de los ciber ataques es lograr la identificación cierta del origen. Como ya se ha demostrado en capítulos anteriores, el limbo jurídico o falta de legislación internacional que facilite la investigación de los causantes de ciber ataques, se encuentren donde se encuentren; las características técnicas intrínsecas del ciber espacio; la guerra de baja intensidad; la presencia o coincidencia de actores de diferente índole: estados, grupos organizados con motivación política o económica, individuos particulares, atacantes secuestrados que desconocen que sus equipos están siendo usados para realizar acciones maliciosas; son verdaderos obstáculos para llegar a atribuir un ataque a un Estado, grupo o individuo.

   En los conflictos tradicionales la crisis se desata entre dos estados claramente definidos –enemigo convencional–. Con la irrupción del terrorismo a gran escala y las actividades en el ciber espacio en la frontera entre lo militar y lo delictivo; la amenaza en muchos casos no tiene cara o una identificación clara y evidente –enemi-

(117) La guerra de baja intensidad es una confrontación político militar entre Estados o grupos, por debajo de la guerra convencional y por encima de la competencia pacífica entre naciones. Involucra a menudo luchas prolongadas de principios e ideologías y se desarrolla a través de una combinación de medios políticos, económicos, de información y militares.

(118) Para más información, ver segunda conferencia «Cyber Warfare: as a form of Low-Intensity Conflict and Insurgency» en la referencia bibliográfica 1.

go asimétrico–. Actualmente la OTAN trabaja considerando todos los casos posibles, amenaza convencional, amenaza asimétrica y amenaza híbrida, la amenaza derivada de la confluencia de acciones convencionales con acciones asimétricas.
Otro hecho relevante a la hora de la toma de decisión de una intervención militar es el hecho evidente de que los límites entre las competencias militar y policial son cada vez más borrosos.

4. ¿Sería aceptable una respuesta tardía?
   En un caso de conflicto convencional o nuclear la respuesta del país atacado se produciría en caliente, es decir inmediatamente después de recibir el ataque y esto sería claramente aceptado por la comunidad internacional de acuerdo al derecho de legítima defensa establecido en el art. 51 de la carta de las Naciones Unidas.
   En el caso de un ciber conflicto de gran escala y en caso de llegar a una atribución clara e inequívoca del atacante, esto llevaría un tiempo que en muchos casos sería de varios meses y esto haría que la respuesta pueda ser entendida más como una represalia que como legítima defensa.

La amenaza cibernética y el artículo 6 del tratado de Washington

El artículo 6 del tratado de Washington dice:

> *«A efectos del artículo 5, se considerará ataque armado contra una o varias de las Partes, el que se produzca:*
>
> *a) Contra el **territorio** de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer.*
>
> *b) b) Contra las **fuerzas, buques o aeronaves** de cualquiera de las Partes que se hallen en estos territorios, como en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer.»*

En el caso de la aplicación del artículo 6, estamos ante la disyuntiva de saber qué se entiende por territorio o por fuerzas en el caso de un conflicto en el ciberespacio.

Conclusiones

La OTAN debe hacer un esfuerzo de renovación de acuerdo al tipo de amenaza al que se enfrenta en la actualidad y al que se enfrentará en el futuro; y eso pasa por considerar el hecho cibernético en: a) la definición de conceptos, estrategias, doctrinas y procedimientos; b) en sus formas de actuación y c) en su ámbito de influencia internacional; consolidando colaboraciones y acuerdos entre la OTAN y Estados No-OTAN, el sector privado y organizaciones no gubernamentales. La OTAN está en ello.

BIBLIOGRAFÍA

Conference on Cyber Conflcit, Proceedings 2010. **Czosseck, Christian; Podins, Karlis;.** Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010. ISBN 978-9949-9040-1-3.

The Virtual Battlefield: Perspectives on Cyber Warfare. **Czosseck, Christian; Geers, Kenneth;.** Tallinn: IOS Press BV, 2009. ISBN 978-1-6750-060-5.

Tikk, Eneken; Kaska, Kadri; Vihul, Liis;. *International Cyber Incidents, Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.

Frameworks for international cyber security. **Tikk, Eneken.** Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.

Coleman, Kevin G. *Cyber Commander's Handbook, the Weaponry & Strategies of Digital Conflict.* Pittsburgh, PA: Technolytics, 2010. ISBN 978-0-578-03935-02995.

Pastor Acosta, Oscar; Pérz Rodríguez, José Antonio; Arnáiz de la Torre, Daniel; Taboso Ballesteros, Pedro;. *Seguridad Nacional y Ciberdefensa.* Madrid: Cátedra ISDEFE-UPM, 2009. ISBN 978-84-7402-364-0.

(SEMA), Sweedish Emergency Management Agency. *Large Internet Scale Attack.* Stockholm: Sweedish Emergency Management Agency (SEMA), 2008. ISBN 978-91-85797-14-1.

Heickerö, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Stockholm: Sweedish Defence Reserach Agency, 2010. ISSN 1650-1942.

Ottis, Rain. *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2008.

CAPÍTULO QUINTO

LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR

LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR

JUAN JOSÉ DÍAZ DEL RÍO DURÁN

RESUMEN

Este capítulo estudia la ciberseguridad en el ámbito militar. Para ello, se comienza dando un enfoque general de estrategia, referido a los nuevos retos y amenazas del comienzo del siglo XXI, para pasar a continuación a analizar los riesgos en el ciberespacio y el estado del arte de la defensa, explotación y ataque en esta nueva dimensión, considerada un nuevo «global common». Se repasa asimismo, la necesidad de introducir nuevas perspectivas en el concepto estratégico de la OTAN ante el papel cada vez más relevante de esta dimensión y se describen las actuaciones y medidas tomadas, tanto por otros países de nuestro entorno como por nuestro Ministerio de Defensa para afrontar este desafío y la estructura y organización adoptada. Se finaliza examinando el importante esfuerzo de colaboración internacional en este campo del Ministerio de Defensa, así como las numerosas actividades de formación, concienciación y adiestramiento desarrolladas en el ámbito del EMAD, concluyendo con un análisis de la cifra y su industria en España.

Palabras clave: Estrategia, amenazas, riesgos, políticas, seguridad, información, ciberespacio, redes, internet, comunicaciones, tecnología, ciberseguridad, ciberdelincuencia, ciberataque, ciberdefensa, ciberterrorismo, ciberguerra, Rusia, China, vulnerabilidad, inteligencia, dimensión, global, NEC, CNO, OTAN, enemigo, Ministerio de Defensa, normativa, organización, mando, control, infraestructura, cooperación, adiestramiento, formación, concienciación, cifra.

CYBER-SECURITY IN THE MILITARY FIELD

ABSTRACT

This chapter examines the cyber-security in the military field. To this end, it starts giving a general approach of strategy, referred to the new challenges and threats at the beginning of this century, analyzing then the risks in cyberspace and the state of the art of the defense, exploitation and attack in this new dimension, considered a new «global common». It looks in addition, the need to introduce new prospects in the strategic concept of NATO facing the role increasingly relevant to this dimension and describes the actions and measures taken, both by other countries in our environment and our Ministry of Defense to cope with this challenge and the structure and organization adopted to do it. It finishes taking consideration on the important international collaborative effort in this area of the Ministry of Defense, as well as the numerous training activities, awareness and training efforts developed in the field by the Defense Staff, concluding with an analysis of the encryption methods and technologies and its industry in Spain.

Key words: Strategy, threats, risks, policies, security, information, cyberspace, networks, Internet, communications, technology, cyber-security, cyber crime, cyberattack, cyberdefence, cyberterrorism, ciberwarfare, enemy, Russia, China, vulnerability, intelligence, dimension, global, NEC, CNO, NATO, Ministry of Defense, regulations, organization, command, control, infrastructure, cooperation, training, education, awareness, encryption.

INTRODUCCIÓN

Miércoles 2 de mayo de 2007; Redmond (Estado de Washington, Estados Unidos); Sede de Microsoft; reunión organizada por la NATO Office of Security y el Departamento de Defensa de EEUU con la colaboración del gigante de la informática; es la séptima edición del «NATO Cyber Defense Workshop». Están presentes la mayor parte de los representantes de las naciones OTAN en asuntos de seguridad en el ciberespacio. Todo transcurre según lo previsto. Es el momento de que el representante del Centro de Excelencia de Ciberdefensa de la OTAN en Tallin (Estonia), el Profesor Peeter Lorents, presente los progresos en la constitución del Centro.

La información con la que comienza su intervención nos deja perplejos y se abre un gran debate. Acaba de decirnos que su país está siendo objeto de ataques cibernéticos desde el día 27 de abril, al principio sencillos, mal coordinados y fácilmente mitigables, pero que desde el día 30 eran más sofisticados y mejor coordinados y se centraron en ciertos routers y DNS (Domain Name Servers) causando interrupciones temporales del servicio al mayor proveedor de comunicaciones fijas de Estonia.

Una novela de ficción podría empezar así, pero desafortunadamente los hechos que se describen arriba son reales y ocurrieron tal y como se ha descrito. Sin embargo y a pesar de que posiblemente esa línea atraería con mayor fuerza la atención del lector, creo que este capítulo debe redactarse de una forma convencional y estructurada. Para ello intentaré hacer en primer lugar un enfoque estratégico general, pasando a continuación a particularizar en la ciberseguridad.

Escenario estratégico general

El escenario estratégico del comienzo de este siglo XXI, se caracteriza porque, junto a los tradicionales riesgos y amenazas para la paz, el equilibrio, la estabilidad y la seguridad internacionales, han emergido otros de nuevo cuño, como el del terrorismo de carácter transnacional y alcance global, con gran capacidad de ocasionar daño indiscriminadamente, así como las diferentes modalidades de ataques que se pueden producir a través del ciberespacio.

Los atentados de Nueva York, Madrid o Beslán, en cuanto al terrorismo y los ciberataques sobre Estonia, Georgia y un largo etcétera de países, en cuanto al ciberespacio, han evidenciado que, frente a los nuevos riesgos y amenazas, la superioridad militar tradicional no constituye un factor de disuasión eficaz ni garantiza más seguridad automáticamente. Tampoco asegura una prevención efectiva contra ataques terroristas o ciberataques, ni evita el riesgo de proliferación de armas de destrucción masiva, cuya posibilidad de caer en manos de tales grupos es hoy la amenaza más grave para la seguridad global.

La lucha contra estas nuevas amenazas es clave en la estrategia de las organizaciones internacionales de seguridad y defensa. También Europa debe afrontarlas decididamente si no quiere convertirse en un objetivo fácil.

Por vez primera en la historia, la Unión Europea se ha dotado de una estrategia de seguridad propia. Pero ésta reclama una mayor determinación, recursos suficientes y un uso más eficaz y coherente de cuantos instrumentos dispone para la gestión de crisis y la prevención de conflictos; unos requerimientos realmente exigentes a los que ningún país europeo, e incluso EEUU como gran potencia, es capaz de hacer frente en solitario.

A su vez, la Alianza Atlántica, que fue la primera en percibir la necesidad de acomodar las respuestas tradicionales al nuevo escenario estratégico, está inmersa en un proceso de transformación profunda de sus estructuras, procedimientos y capacidades, con el fin de conseguir unas fuerzas aliadas mejor dotadas, interoperables y capaces de actuar con la máxima eficacia.

Nos encontramos, pues, dentro de un nuevo escenario estratégico en el que la política de seguridad demanda planteamientos novedosos y cambios de mentalidad, de un modo especial en lo que se refiere a la gestión de crisis y resolución de conflictos y a la necesidad de adaptación de las Fuerzas Armadas a las circunstancias de cada momento.

El ciberespacio y la ciberseguridad

La alta dependencia tecnológica de nuestra sociedad es una realidad constatable, siendo imprescindible para el buen funcionamiento de los Estados, sus Fuerzas y Cuerpos de Seguridad y sus infraestructuras. Esta dependencia seguirá aumentando en el futuro. Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera. Todas estas funciones dependen de sus redes de comunicaciones e informáticas, que en el caso de EEUU, por ejemplo, consisten en más de 15.000 redes(1) y siete millones de terminales informáticos distribuidos en cientos de instalaciones en docenas de países, para cuyo funcionamiento mantienen más de 90.000 especialistas. En menos de una generación, las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico.

(1) www.afcea.org/signal/signalscape/index.php/2010/08/cyberdefense-issues-dod-culture/;
www.reuters.com/article/idUSTRE69C5ED20101013

Paralelamente, la dependencia tecnológica, la globalización y la facilidad de acceso a las tecnologías hace que a día de hoy la probabilidad de sufrir ataques informáticos o ciberataques sea muy elevada, permitiendo potencialmente a nuestros adversarios obtener inteligencia valiosa de nuestras capacidades y operaciones y desestabilizar nuestra economía. Como es lógico, a mayor dependencia, mayor es el impacto que podría tener un ataque a los sistemas sobre los que se sostiene un país o una organización.

Los usuarios de Internet se han acostumbrado a pensar que la información de cualquier lugar o suceso de actualidad en el mundo está disponible prácticamente de inmediato, ven el mundo como un gigantesco PC en el que ellos, mediante su «ratón», intervienen de forma interactiva a través del ciberespacio en todas sus actividades (viajes, trabajo, banca, compras, etc). A este respecto, es conocido el pasaje de un relato de Clay Shirky (2), en que un padre le pregunta a su hija mientras están viendo una película en la TV, por qué está buscando algo en la parte trasera de ésta y ella le contesta que «el ratón, porque quiero cambiar el final de la película».

Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar, aire y espacio, a través del ciberespacio. Citemos a continuación algunos datos que nos pueden dar una dimensión del problema:

- Si en diciembre de 1.995 el número de usuarios de Internet era de 16 millones, en 2.001 pasó a ser de 458 millones y en enero de 2010 alcanzó la cifra de 1.700 millones (3). Se espera que en 2.015, el número de terminales con acceso a Internet supere el número de habitantes de nuestro planeta (4).
- Durante 2008, Symantec creó 1,6 millones de nuevas firmas de amenaza, o lo que es lo mismo, una nueva firma cada 20 segundos (5).

---

(2) Clay Shirky (nacido en 1964) es un escritor americano, consultor y profesor sobre los efectos sociales y económicos de las tecnologías de Internet. Enseña Nuevos Medios de Comunicación en la Universidad de Nueva York (NYU).

(3) www.internetworldstats.com/stats.htm

(4) W.D. Sincoskie, Telecordia Technologies.

(5) Enlace: www.symantec.com/business/resources/articles/article.jsp?aid=20090511_symc_malicious_code_activity_spiked_in_2008.

- La Base de Datos Nacional de Vulnerabilidades de EEUU (The National Vulnerability Database, NVD) (6), integra todas las vulnerabilidades disponibles públicamente y contiene aproximadamente 43.800 de ellas a fecha de finales del mes de septiembre de 2.010, así como las alertas del US_CERT (Computer Emergency Response Team), catalogando aproximadamente 13 al día.

La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias.

Sun Tzu (600 años a.C.) decía en su obra «El arte de la guerra»: «Cien victorias en cien batallas no es lo ideal. Lo ideal es someter al enemigo sin luchar». Este pensamiento ha ganado valor con el paso del tiempo, especialmente con el nacimiento del ciberespacio y la ciberguerra. Puede ser la primera ocasión en que su pensamiento podría imaginarse realizado en toda su extensión gracias a la existencia del ciberespacio. El ciberespacio es una nueva dimensión en la que se pueden materializar conflictos y guerras, que no tiene límites ni fronteras y que, sorpresivamente, parece no tener restricciones ni leyes, al menos efectivas. Por otra parte, Clausewitz pensaba que «La Guerra es un acto de fuerza para doblegar la voluntad del enemigo». Podría deducirse que la ciberguerra aúna los dos pensamientos de estos grandes estrategas, ya que produciendo una parálisis estratégica, se puede doblegar la voluntad del enemigo sin aplicación de la fuerza física.(7)

Ejemplo reciente del lugar preeminente que está ocupando el ciberespacio y su seguridad en nuestro mundo han sido las consecuencias de los ciberataques sufridos por Estonia en el año 2007, del que se hablará con posterioridad. En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes. Este fue el caso de los ciberataques sufridos por Georgia

(6) http://nvd.nist.gov/

(7) «Cyber Wars: A Paradigm Shift from Means to Ends». Autor: Amit Sharma, del Institute for System Studies and Analysis» del Ministerio de Defensa de la India.

durante el conflicto con Rusia en Ossetia del Sur y Abkhazia. Por primera vez en la historia una operación militar fue acompañada de una serie de ciberataques a los sitios Web del gobierno Georgiano y otras páginas comerciales, dejándolos fuera de servicio en algunos casos y modificando el aspecto de las páginas en otros («Defacement»(8)). Expertos de Estados Unidos han concluido que países como China, Rusia o Corea del Norte disponen de unidades especializadas y personal capacitados para llevar a cabo ciberataques y prevén que en los próximos diez años se sufrirán graves consecuencias derivadas de sus acciones, dado que en la actualidad la mayor parte de los sistemas disponen de una protección insuficiente, de procedimientos inadecuados y de un adiestramiento deficiente en seguridad. En este sentido, también se ha pronunciado en febrero de 2010 el antiguo Director de Inteligencia Nacional de EEUU, Mike McConnell (9); afirmó ante el Comité de Ciencia, Transporte y Comercio del Senado, que «el país no se está tomando con seriedad la ciberseguridad y caerá víctima de un ciberataque demoledor en los próximos años. Si la nación entrara en una ciberguerra, perderíamos… no mitigaremos este riesgo. Hablaremos de ello, agitaremos los brazos, tendremos una ley, pero no vamos a mitigar este riesgo». McConnell dijo también declararse fuerte partidario de que el gobierno asuma un papel principal en la ciberseguridad, ya que un ciberataque importante podría paralizar el comercio y hacer temblar la confianza de los consumidores en los mercados financieros y el gobierno federal, «compitiendo con los daños de un ataque nuclear al país».

Las posibles consecuencias de este tipo de ataques pone de relevancia la necesidad de dotarse de una capacidad de seguridad en el ciberespacio, que garantice una adecuada protección frente a éstos y que a su vez permita conocer y bloquear los sistemas del adversario en caso necesario. En países aliados y de nuestro entorno ya se han iniciado los trabajos para obtener esta capacidad. La situación podría agravarse con la actual crisis económica, ya que ésta está originando una restricción en

(8) ***Defacement*** es un término usado en *informática* para hacer referencia a la deformación o cambio producido de manera intencionada en una *página web* por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún *bug* en el propio *servidor* o por una mala administración de éste. Ataques de defacement conocidos se han hecho sobre los portales de Twitter por el «ciberejército iraní», en el de nuestra última presidencia de la UE y en los de los gobiernos de Georgia y Venezuela, este último «colgando» un recordatorio de la «*boda*» entre los señores Castro y Chávez.

(9) www.federaltimes.com/article/20100224/IT01/2240307/-1/RSS

inversiones de seguridad tanto en empresas como en las administraciones públicas y las FAS.

En Estados Unidos la seguridad en el ciberespacio está al mismo nivel que el «Homeland Security», habiendo nombrado el actual gobierno de Obama, un coordinador de ciberseguridad en la Casa Blanca, que será responsable de supervisar una estrategia nacional para garantizar los intereses de los americanos en el ciberespacio. En el ámbito militar americano, ya desde hace unos años, se han llevado a cabo trabajos para la obtención de una capacidad de Operaciones en el Ciberespacio en cada uno de los ejércitos. Posteriormente, explicaré los objetivos de estas Operaciones.

En Alemania, se ha formado la «Unidad de Reconocimiento Estratégico del Bundeswehr», compuesta por un numeroso grupo (10), en su mayoría expertos en seguridad y en el Reino Unido se ha creado una Oficina de Ciber Seguridad (OCS, Office of Cyber Security) encargada de coordinar las capacidades defensivas y de respuesta a intrusiones en redes del Reino Unido (11). El ex-Primer Ministro Gordon Brown, declaró que «de la misma forma que en el siglo diecinueve tuvieron que asegurar los mares por su seguridad nacional y prosperidad y en el veinte fue el espacio aéreo, en este siglo toca hacerlo con el ciberespacio para que los negocios y las personas puedan operar de modo seguro en él».

Hace un año, el Presidente Obama declaraba; «Dado el enorme daño que puede causar incluso un único ataque cibernético, no bastará con respuestas a medida. No es suficiente el reforzar nuestras defensas tras los incidentes o ataques. De igual forma a cómo hacemos frente a los desastres naturales, hemos de tener planes y recursos de antemano, compartiendo información, emitiendo avisos y asegurando una respuesta coordinada». (Presidente Barack Obama, 29 mayo 2009).

A nivel nacional, el Ministerio de Defensa ha publicado la Política de Seguridad de la Información, sus normas de aplicación y ha tomado numerosas iniciativas para incrementar la seguridad de su información, tanto en el ámbito de la red de Propósito General (de orientación administrativa) como en el de Mando y Control (dependiente del JEMAD y orientado a las operaciones). Como es lógico, también la Directiva de

(10) www.spiegel.de/international/germany/0,1518,606987,00.html

(11) www.securecomputing.net.au/News/148634,uk-government-to-create-office-of-cyber-security.aspx.

Planeamiento Militar estudia las capacidades relacionadas con el ciberespacio con las que las Fuerzas Armadas deben contar y el Concepto de Estrategia Militar, describe el nuevo escenario estratégico, en el que la ciberseguridad es tenida en cuenta y se analizan las tendencias y previsiones en este campo.

El JEMAD también ha expresado públicamente la importancia del desarrollo de capacidades relacionadas con las nuevas tecnologías, resaltando la necesidad de desarrollar medidas para mejorar la seguridad de los aliados ante la posibilidad de un ciberataque y definiendo esta amenaza como una de las más complejas a la que cualquier sistema defensivo puede enfrentarse, tanto por sus potenciales efectos sobre la sociedad como por su dificultad de identificar al agresor (12).

La ciberguerra es asimétrica. El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares. Unos cuantos programadores pueden, si encuentran una vulnerabilidad a explotar, amenazar nuestros sistemas logísticos, robar nuestro planeamiento operacional o cegar nuestros sistemas de inteligencia y de mando y control. Por este motivo, muchos ejércitos están desarrollando capacidades ofensivas en el ciberespacio y se estima que más de 100 servicios de inteligencia extranjeros llevan a cabo estas actividades (13). Para tratar de impedirlo y estar por delante de nuestros adversarios, necesitamos ajustar y mejorar continuamente nuestras defensas. Por otra parte, el análisis forense necesario para identificar a un atacante puede llevar meses, si es que la identificación es posible finalmente, e incluso, si el atacante es identificado y no es un estado sino por ejemplo, un grupo terrorista, puede suceder que no tengamos medios para responder. Para más complicación, los ciberataques a menudo se originan en servidores situados en países neutrales y las respuestas pueden conllevar consecuencias imprevistas a sus intereses, razón por el que el uso de este tipo de reacciones debe estar siempre bajo un mando estratégico que tenga una visión integral y global de la situación.

Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados; tanto su software como su hardware pue-

(12) www.uimp.es/blogs/prensa/2009/07/17/el-jemad-afirma-que-no-hay-alternativas-claras-a-la-otan-porque-hoy-por-hoy-es-una-alianza-insustituible/
(13) www.reuters.com/article/idUSTRE69C5ED20101013

den ser saboteados antes de ser unidos en un sistema en explotación. El código dañino, incluyendo las «bombas lógicas (14)», puede insertarse en el software cuando se está desarrollando. En cuanto al hardware, tanto las «puertas traseras», como los «kill switches (15)», se pueden «grabar» en el «firmware» de los «chips» de los ordenadores, permitiendo su manipulación remota: el riesgo de manipulación en el proceso de fabricación es totalmente real y es la menos comprendida de las ciberamenazas. El sabotaje es prácticamente imposible de detectar y peor todavía de erradicar. Este tipo de amenaza ya se ha materializado en hardware adquirido por el DoD de EEUU y con seguridad en el de muchos otros países que no han sido capaces de detectarlo.

Ejércitos de diversos países han reconocido formalmente al ciberespacio como un nuevo dominio de enfrentamiento («Global Commons (16)»). Aunque el ciberespacio es un dominio hecho por el hombre, se ha hecho tan crítico para las operaciones militares como la tierra, el mar, el aire y el espacio.

Tanto la OTAN, como la UE están llevando a cabo acciones para dotarse de una capacidad que les permita defenderse y reaccionar adecuadamente frente a estas amenazas. En la Declaración de la Cumbre de Riga (29 de noviembre de 2006), los Jefes de Estado y de Gobierno de la OTAN demandaron la mejora de la protección de los sistemas de información claves respecto de posibles ciberataques. En la Declaración de la Cumbre de Estrasburgo (4 de abril de 2009), afirmaron la vigencia

(14) Es una parte de código insertada intencionadamente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre-programadas, en cuyo momento se ejecuta una acción maliciosa. Por ejemplo, un programador puede ocultar una pieza de código que comience a borrar archivos cuando sea despedido de la compañía (en un disparador de base de datos, «trigger», que se dispare al cambiar la condición de trabajador activo del programador).

(15) Es una medida de seguridad utilizada para apagar un dispositivo en una situación de emergencia en la que no se puede hacer de la forma habitual. Al contrario que en un apagado normal, que cierra todos los sistemas de forma ordenada y sin dañar la máquina, un «kill switch» está diseñado para abortar completamente la operación a cualquier coste.

(16) Se conocen como «Global Commons», aquellos entornos en los que ninguna persona o estado puede tener su propiedad o control y que son básicos para la vida. Un «Global Common» contiene un potencial infinito en lo referente al conocimiento y avance de la biología y la sociedad. Incluye los mares, el aire, el espacio y el ciberespacio. www.twq.com/10july/docs/10jul_Denmark.pdf («Managing the global Commons», por Abraham M. Denmark).

de su compromiso en el fortalecimiento de los sistemas de información y comunicaciones de importancia crítica para la Alianza frente a ciberataques, que tanto agentes estatales o no, pueden tratar de explotar, pues cada vez es mayor la dependencia de estos sistemas. A modo de ejemplo, la OTAN, aparte de adquirir la correspondiente capacidad, NCIRC (NATO Computer Incident Response Capability), para cuyos objetivos se basa principalmente en su Centro Técnico y definir el Concepto y Política de Ciberdefensa, ha creado la Autoridad de Gestión de la Ciberdefensa (CDMA, Cyber Defense Management Authority) y su correspondiente estructura y organización de apoyo; La ciberseguridad es uno de los desafíos más importantes a la seguridad, siendo un asunto estratégico del mismo nivel que las Armas de Destrucción Masiva y la Yihad Global(17). Por otra parte, la UE ha elaborado el Concepto de Operaciones en Red (CNO; Computer Network Operations) y la EDA (European Defence Agency) ha publicado el correspondiente contrato para su implementación(18). EE.UU ha creado un Mando para el Ciberespacio (Cyber Command).

Las operaciones cibernéticas en redes (CNO; Computer Network Operations)

El término «CNO» tiene una amplia acepción, tanto en el campo civil como militar. En su sentido militar, se podría definir como las acciones tomadas de forma deliberada para obtener la superioridad en la información y denegarle ésta al enemigo. La superioridad en la información es un elemento clave en el concepto NEC (Network Enabled Capability), que trataremos en el siguiente apartado. Dentro del dominio militar, se considera una de las cinco capacidades principales de las Operaciones de Información (IO), junto con las conocidas en el mundo anglosajón como: Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC) y Electronic Warfare (EW).

Las CNOs, en combinación con las de Guerra Electrónica (EW), se utilizan principalmente para interrumpir, perturbar, inutilizar, degradar o engañar los sistemas de mando y control del enemigo, anulando su capacidad para tomar decisiones con eficacia y oportunidad, preservando

(17) www.betanews.com/article/Mr-Obama-Dont-forget-the-cyberwar-threat/1228782845

(18) B-Brussels: 'computer network operations for EU-led military operations (EU milops CNO capability)' — 10-CAP-OP-37 2010/S 157-242011 Contract notice. www.eda.europa.eu/genericitem.aspx?area=Reference&id=665)

a la vez los sistemas de mando y control propios y amigos. Las CNOs, de acuerdo con la publicación Joint Doctrine for Information Operations de EEUU (19), se subdividen a la vez en tres:

- Computer Network Defence (CND), que incluye las acciones tomadas para proteger, monitorizar, analizar, detectar, reaccionar y recuperarse frente a los ataques, intrusiones, perturbaciones u otras acciones no autorizadas que podrían comprometer la información y los sistemas que la manejan.
- Computer Network Exploitation (CNE), que incluye las acciones e inteligencia de recolección de información sobre sistemas de información enemigos, así como su explotación.
- Computer Network Attack (CNA): que incluye las acciones tomadas para perturbar, denegar, degradar o destruir información que circula por los sistemas enemigos.

NNEC (NATO Network Enabled Capability)

La era de la información está alterando la distribución de poder, aumentando la complejidad de los sistemas CIS, restando importancia a las distancias geográficas y reduciendo drásticamente los tiempos de reacción.

Estos cambios, así como las recientes operaciones en curso, están llevando a todos los Aliados a transformar las Capacidades de sus FAS (Fuerzas Armadas), donde una red de redes dentro del concepto NEC (Network Enabled Capability), que definiremos en breve, jugará un factor decisivo en las operaciones y se potenciará como motor y guía de nuestro esfuerzo, alcanzándose la Superioridad en la Información.

Para que el Mando pueda decidir y la decisión a tomar sea la correcta y adecuada para la conducción de las operaciones, esa información habrá de ser precisa, fiable, pertinente y oportuna. En una primera aproximación y de forma general (sin particularizar en el caso OTAN), se podría decir que NEC es «la capacidad de integrar todos los componentes del medio operativo (sensores, elementos de decisión y plataformas de armas) desde el nivel político-estratégico hasta el nivel táctico, a través de una infraestructura de información y redes».

(19) www.c4i.org/jp3_13.pdf, http://www.au.af.mil/info-ops/netops.htm, www.iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm

Formalmente, se conoce como NNEC «la capacidad cognitiva y técnica de la Alianza para federar los diferentes componentes del entorno operativo, desde el nivel estratégico hasta el táctico, mediante una infraestructura de redes y sistemas de información». Trataremos de ver lo que este concepto significa desde la óptica de la seguridad de la información, que es uno de los mayores retos a los que nos enfrentaremos en la convergencia hacia esta nueva capacidad de operación en red.

Los principios(20) de NNEC son los siguientes: una Fuerza robustamente conectada mejora el conocimiento compartido de la información. Compartir la información mejora la calidad de ésta y la percepción de la situación. La percepción compartida de la situación permite la colaboración y sincronización y mejora la velocidad de decisión del Mando, lo que a su vez, incrementará enormemente la eficiencia de las misiones por la agilidad y velocidad de la acción. NNEC busca la mejora de la eficiencia de la toma de decisiones, mediante la integración de las personas y la información en una red.

La gestión de la información en NNEC será una responsabilidad fundamental, que requiere liderazgo, involucración de máximo nivel y la creación y mantenimiento de una estructura organizativa eficaz. La información se gestionará haciendo hincapié en la «responsabilidad de compartir» («responsibility-to-share») convenientemente equilibrada con el principio de seguridad de la «necesidad de conocer» («need-to-know»). La información se protegerá de acuerdo con los principios de «Seguridad de la Información» («Information Assurance»), es decir, de su confidencialidad, integridad, disponibilidad, autenticidad y no repudio.

Todo usuario tendrá un perfil de derechos de acceso a la información, dondequiera que se conecte a la federación de redes. Aunque habrá ocasiones en que las naciones no querrán compartir ciertas informaciones, esto será la excepción, no la regla.

La convergencia a NEC exigirá una prácticamente total interconexión con otros sistemas (Federación de Redes), incluso con ONGs. Este puede ser el caso de la AMN (Afghanistan Mission Network) (21), que constituye una federación de redes entre la red clasificada de ISAF (Internatio-

---

(20) www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf, *nnec.act.nato.int/, www.afcea.org/.../060525-AFCEA2006DraftV1.2.pptMajGenvanDam_000.ppt* y *www.bdcol.ee/.../7_%20Arturas%20Litvaitis-Challenges%20of%20Implementing%20NCW%20Tenets%20in%20Coaliti...*

(21) www.isaf.nato.int/

nal Security Assistant Force) y las extensiones nacionales de las redes de los países de la Coalición(22), con todas las medidas de seguridad que esto conlleva a fin de minimizar los riesgos. Como podemos fácilmente deducir de todo lo anteriormente citado, el esfuerzo (sobre todo en el aspecto de seguridad) para poder alcanzar todos los objetivos citados será muy considerable y requerirá no solamente importantes recursos técnicos, humanos y económicos, sino también un cambio de mentalidad imprescindible. Los principales retos serán:

- Todos los usuarios precisarán recibir la formación y adiestramiento adecuados para utilizar adecuadamente la cada vez mayor información disponible. Necesitarán emplear todas las herramientas disponibles del sistema para extraer la información y necesitarán tiempo para adaptarse a un tipo de cultura más abierta, que requiere compartir la información en mucho mayor grado y establecer la confianza entre los colegas y socios de las coaliciones que se determinen.
- Los desafíos técnicos y procedimentales no deben tampoco ser subestimados. La capacidad de desarrollo será a menudo compleja y requerirá la integración de sistemas legados y sistemas nuevos, a la vez que será necesario asegurar las actualizaciones futuras a todo el sistema en su conjunto. Todo esto conllevará unos procesos de adquisición más flexibles y la búsqueda de socios adecuados en la industria.
- Mientras que la mayoría de nuestros aliados pondrán su capacidad militar en NEC, habrá algunos socios de coalición y organizaciones que no estarán en sintonía, lo que requerirá una consideración profunda de este problema para poder trabajar con ellos.
- Todos estos desafíos vendrán acompañados por la necesidad de evitar una sobrecarga de información y garantizar la robustez de la red. La cada día más creciente amenaza de los ataques cibernéticos, a la que seremos más vulnerables a medida que crezca nuestra dependencia de la red, hará que debamos paliarla mediante nuevas medidas de seguridad. Habrá que tener previsto el poder continuar las actividades en modo degradado y evitar el colapso de la red, contando con medios alternativos de comunicación para mantener activos los elementos clave de la red de redes.
- Por último y no por ser lo último tendrá menos importancia, las restricciones presupuestarias obligarán a una cuidadosa priorización en las decisiones de inversión.

(22) www.defensesystems.com/articles/2010/09/02/c4isr-2-afghan-mission-network-connects-allies.aspx

Revisión del concepto estratégico de la OTAN. Ciberespacio y el artículo V

El actual Concepto Estratégico de la OTAN data de 1.999. La Alianza opera en un ambiente de cambio continuo, con desafíos globales, que obligan a su revisión. Se espera que antes de que finalice el año 2010 se establezca el nuevo Concepto (23). Los adversarios pueden intentar explotar la creciente dependencia de la Alianza de los sistemas de información mediante operaciones de información diseñadas para interrumpir, modificar, o interceptar la información manejada en ellos, en una estrategia para contrarrestar la tradicional superioridad de armamento de la OTAN.

Mientras que el Concepto de 1.999 entiende la defensa colectiva bajo el artículo V como la detención del avance del agresor asegurando la independencia política e integridad territorial de sus estados miembros, el nuevo Concepto debería reconocer la necesidad de modificación de la definición de «ataque armado». Parece necesario que la OTAN entienda que un ataque armado puede incluir un acto agresivo en su territorio o fuera de él, tanto en el entorno real como el virtual, si afecta a los intereses vitales de la Alianza.

Al ser la tecnología cada vez más accesible y de menor coste, los adversarios podrían atacar a los miembros de la Alianza, sus centros de comercio y la economía global, incluyendo las redes sociales mediante el necesario pero vulnerable «global common» que las sociedades modernas utilizan para conectarse y prosperar: el ciberespacio. La OTAN debería desarrollar estrategias, políticas y capacidades que le permitan defenderse y responder a las amenazas emergentes en estas áreas.

La Amenaza

En un principio, la mayoría de los llamados hackers no tenían otro tipo de motivos más que los intelectuales para la penetración en las redes. Buscaban popularidad y notoriedad por haberse saltado las medidas defensivas de sistemas importantes. No obstante, hubo un cambio radical cuando surgió la ciberdelincuencia, ya que las motivaciones pasaron a tener como objetivo principal el beneficio económico de forma ilegal; hoy en día se ha desarrollado de forma alarmante. El robo de identidad,

(23) www.nato.int/strategic-concept/what-is-strategic-concept.html

el fraude financiero (en particular la banca online y tarjetas de crédito/débito), el robo de información y ataques diversos para la extorsión son diferentes formas de ciberdelincuencia que se han convertido en un problema muy importante en todo el mundo.

El ciberterrorismo es otra de las amenazas que han cobrado fuerza durante los últimos años, gracias a su evolución y aumento de actividad. Se considera que la capacidad técnica se ha incrementado considerablemente y que la posibilidad de que se puedan lanzar ataques que logren dañar seriamente elementos de las infraestructuras críticas nacionales se ha de tener en cuenta.

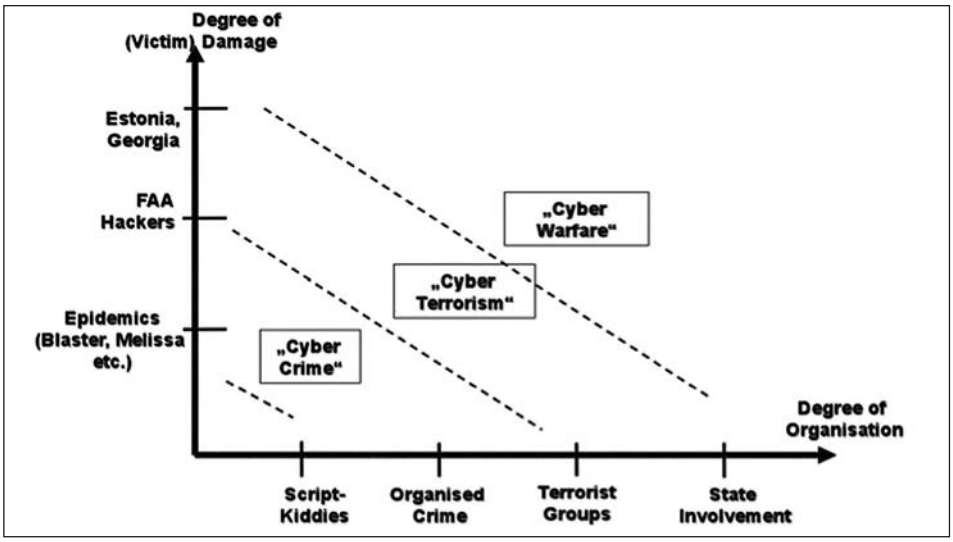
La Yihad Global se apoya en dos pilares: en el plano operativo en los ataques suicidas y en el de gestión, en Internet y en el ciberespacio. Las tres componentes necesarias para el éxito de una operación, incluidas las terroristas (mando, control y comunicaciones), las llevan a cabo a través de Internet. El ciberespacio es también la principal herramienta de propaganda, distribución de ideas, reclutamiento de voluntarios y recaudación de fondos de los terroristas islámicos.

Otra de las amenazas más importantes que se está materializando en este momento es el ciberespionaje. Algunos países, como China (24) y Rusia (25), han hecho de él una extensión de sus metodologías de espionaje clásicas. A partir de estas técnicas pueden adquirir información confidencial de todo tipo, ya sea proveniente de Estados, sus Ejércitos o información industrial que ofrecerá ventajas competitivas al mejor postor. Un ejemplo es la operación «Titan Rain», que implicaba el intento de obtención de información gubernamental de Estados Unidos y Gran Bretaña desde China y que ocasionó una gran fuga de información. En los últimos años, ha habido diferentes ciberataques a países por motivaciones políticas, como pueden ser los realizados contra Estonia, Georgia, Estados Unidos y Corea del Sur. Esto demuestra la capacidad de ciberataques que han obtenido países como Rusia y China, ganando una superioridad estratégica sobre el resto.

Por último, se cierne sobre nosotros el problema de la ciberguerra o ciberconflicto, ya que en teoría para que se pudiese denominar guerra

(24) Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Autor principal; Byan Krekel (Northrop Gruman Corporation).

(25) www.govsecinfo.com/events/govsec-2010/sessions/wednesday/joyals-general-session.aspx y www.nsci-va.org/WhitePapers/2010-02-Cyber%20Espionage%20-%20Is%20the%20US%20Getting%20More%20Than%20It's%20Giving-final%20v1.pdf



debería haber una declaración previa, que normalmente y en los tiempos actuales, no se suele producir. En la figura anterior, se recoge un interesante diagrama en el que se interpretan los posibles ingredientes que se necesitarían o que servirían para diferenciar la frontera entre los conceptos de ciberdelito, ciberterrorismo y ciberguerra, básicamente determinados por el grado de daño infligido y el grado de organización del atacante. Dentro del grado de daños, vemos la progresión desde un simple «gusano», pasando por los ataques sufridos por la Administración Federal de Aviación de EEUU, hasta llegar a los sufridos por Estonia o Georgia, que no dejan de ser el umbral previo a la ciberguerra; todavía nos queda mucho por ver. En cuanto al grado de organización, la ciberguerra requiere el respaldo de un estado.

Algunos estados han comenzado ya su carrera para la obtención de una capacidad de explotación y ataque, pues se atisban futuros ciberconflictos entre países, siendo el ciberespacio una dimensión más donde combatir, como pueden serlo tierra, mar, aire y espacio. Una gran cantidad de medios informativos(26) recogían a principios de octubre las «discusiones y especulaciones generadas a raíz de la aparición del gusano informático Stuxnet, en especial sobre quién está detrás del ataque y cuáles son sus objetivos».

(26) www.boletindintel.es/BoletinesAyS/Publico/PresentaContenido.php?Fase=1%20&%20Referencia=1343 y www.dintel.org/ También: www.economist.com/realarticleid.cfm?redirect_id=17147862

Según Eugene Karpersky, «este programa dañino no ha sido diseñado para robar dinero, bombardear con spam o acceder a datos personales; ha sido diseñado para sabotear y causar daños en entornos industriales. Mucho me temo que estamos asistiendo al nacimiento de un nuevo mundo. Los 90 fueron la década de los cibervándalos, la década del 2000 fue la de los cibercriminales, y tengo la sensación de que estamos entrando en la nueva era de las ciberguerras y el ciberterrorismo,» concluyó Kaspersky.

Según el Boletín DINTEL, la intención final de este gusano era acceder a sistemas de control industrial Simatic WinCC SCADA, que controlan procesos industriales, infraestructuras e instalaciones. Oleoductos, centrales eléctricas, grandes sistemas de comunicación, navegación aérea y marítima, e incluso instalaciones militares, utilizan sistemas similares. Tanto el blanco del ataque como la geografía donde se han detectado los primeros brotes (principalmente Irán), inducen a pensar que no se trata de un grupo cibercriminal normal. Es más, los expertos en seguridad de Kaspersky Lab, que han analizado el código del gusano, insisten en que el objetivo principal de Stuxnet no ha sido sólo el de espiar sistemas infectados, sino también el de llevar a cabo acciones de sabotaje. Todos estos hechos apuntan al hecho de que es muy probable que algún estado-nación, con acceso a grandes volúmenes de información de inteligencia, haya dado cobertura al desarrollo de Stuxnet.

Las redes de Mando y Control que manejan información clasificada poseen un alto nivel de protección y no están conectadas a Internet: sin embargo, esto no garantiza su seguridad «per se». Todos los SSOO (Sistemas Operativos) y gran número de aplicaciones empleadas en redes clasificadas son COTS (Commercial Off The Shelf), que requieren su actualización continua (especialmente para contrarrestar vulnerabilidades de seguridad), lo que se realiza a través de Internet en servidores separados, pero es prácticamente imposible analizar el código de dichas actualizaciones (a veces suponen millones de líneas de código y el fabricante no publica su contenido), por lo que solamente se suele probar en maqueta su repercusión en los sistemas antes de pasar a explotación.

Por otro lado, todos los «chips» son de manufactura no nacional y éstos pueden incluir en su «firmware» código dañino no detectable o de muy difícil detección. A día de hoy prácticamente la totalidad de los sistemas clasificados disponen de interconexiones a otros sistemas, ya sean OTAN, UE o de países aliados, lo que complica enormemente el

mantenimiento de la seguridad. Por último, tanto la OTAN y EE.UU, por ejemplo, han reconocido e informado de numerosos incidentes de seguridad en sus sistemas clasificados durante los últimos años.

Ataques e incidentes reseñables

Solo comentaré algunos de los incidentes más conocidos para poder situar el alcance de esta amenaza:

EEUU

Tal y como recientemente declaró el Vicesecretario de Defensa de EEUU, el señor William J. Lynn III (27), en la primavera de 2008, una variante de un gusano relativamente «benigno» de tres años de edad, comenzó su sinuoso camino a través de las redes militares clasificadas de EEUU, diseminado por medio de un dispositivo de almacenamiento removible («flash drive USB») introducido en un portátil en una base de Oriente Medio y se autocargó en una red del Mando Central de EEUU. El Pentágono ha afirmado hace unos meses que la penetración, fue un ataque deliberado lanzado por un servicio de información extranjero. El código se diseminó sin ser detectado tanto en redes clasificadas como no clasificadas, estableciendo lo que se puede considerar una «cabeza de playa» digital, desde la que los datos podían transferirse a servidores bajo control extranjero. Este gusano fue una auténtica pesadilla para los administradores de las redes, que necesitaron cerca de 14 meses de trabajo para su limpieza, bajo la operación denominada «Operation Buckshot Yankee» y constituyó el mayor compromiso de la seguridad de las redes militares de EEUU, marcando un punto de inflexión en su estrategia de ciberdefensa, lo que originó que se llevase a cabo una gran reorganización de las fuerzas de defensa de la información, incluyendo la creación del nuevo Mando del ciberespacio (Cyber Command) (28).

El 4 de julio de 2009, día en que se celebra la fiesta de la independencia en Estados Unidos, se sucedieron una serie de ataques de Denegación de Servicio contra diferentes instancias en ese país (la Casa Blanca, el Departamento de Seguridad, el Servicio Secreto, la Agencia

(27) www.cfr.org/publication/22849/defending_a_new_domain.html
(28) www.wired.com/dangerroom/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/#ixzz0zDYjk9kk

de Seguridad Nacional…), llevados a cabo por una red de «botnets» (29) de más de 50.000 ordenadores. Dos días más tarde, esta misma red atacó a otros once objetivos en el gobierno de Corea del Sur. Se concluyó que el autor primario de ambas operaciones era Corea del Norte, siendo los motivos políticos los más probables. Se sabe, además, que la inteligencia militar de este país ha entrenado a un conjunto de hackers para fortalecer su capacidad de ciberataque.

Estonia

Aunque este capítulo comenzaba con una mención a los ataques sufridos por este país, creo necesario dar alguna información complementaria, ya que se puede considerar como el primer ataque serio contra las infraestructuras cibernéticas de una nación. Estonia sufrió un fuerte ciberataque en los meses de abril y mayo de 2007. Fueron una continuación en el ciberespacio de los problemas relacionados con motivo de la retirada del monumento soviético conmemorativo de los soldados caídos durante la Segunda Guerra Mundial. Junto a las manifestaciones y protestas en las calles de Tallin, Estonia sufrió una serie de ataques informáticos que dejaron fuera de servicio los sitios Web del gobierno, bancos, escuelas, etc. durante unos días, requiriéndose el apoyo experto de la OTAN y países aliados para contener los daños. La agitación fue proporcionada por la propaganda rusa, difundida por medios de comunicación y foros de debate de Internet.

Los ataques iniciales del 27 y 28 de abril fueron simples, mal coordinados y fácilmente atenuados; hubo un par de páginas web que sufrieron «defacement» y muchos ataques de denegación de servicio (DDoS) (30) contra servidores web del gobierno. Algunos blancos civiles

(29) **Botnet** es un término que hace referencia a un conjunto de *robots informáticos* o *bots*, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del *IRC*: Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante *HTTP*, con lo que el control de estas máquinas será mucho más simple.

(30) Un **ataque de denegación de servicio**, también llamado ataque **DoS** (de las siglas en *inglés **D**enial **of** **S**ervice*), es un ataque a un sistema de *computadoras* o *red* que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del *ancho de banda* de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le

fueron también atacados, especialmente los portales de noticias. Las descripciones detalladas de ataque, información de objetivos y los datos de tiempo de ejecución fueron albergados en muchos foros de hackers rusos y foros de discusión. La información fue también diseminada vía Chats (charla interactiva) de Internet, MSN y correo electrónico. Algunos sitios también suministraron herramientas de software para atacar los objetivos designados.

El 30 de abril se produjo un cambio en el perfil atacante, cuando empezaron a aparecer programas de ejecución automática (bots) más grandes y ataques bien coordinados. Estos nuevos ataques también se dirigieron a la infraestructura de la red, a los Internet Service Providers (ISPs). Se atacaron también servidores DNS (31) en el ISP, con éxito en algunos casos, afectando a servicios de DNS temporalmente en gran parte de Estonia. Los robots de spam (publicidad/información no deseada) se usaron para atacar servicios de correo electrónico del gobierno con resultados diversos, si bien la mayoría de los sistemas pudieron resistir los ataques.

Ya el cuatro de mayo se produjo el mayor de los ataques. La mayoría de las agresiones eran relativamente «sencillas» y pudieron ser bloqueadas en los ISPs, aunque no obstante, algunos sistemas quedaron tem-

---

dice «denegación», pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz.

(31) Domain Name System / Service (o DNS, en español: sistema de nombre de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

poralmente fuera de servicio. Después de los ataques del 4 de mayo, la situación pareció calmarse.

En la mañana del día 10, el sitio web www.hanza.net (el banco más grande de Estonia) fue blanco de un fuerte ataque de DDoS; más de 97 % de todas transacciones de banco en Estonia son realizadas en Internet. La mayoría de los demás ataques tuvieron poco efecto sobre la población.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y NORMATIVA EN EL MINISTERIO DE DEFENSA

La seguridad de la información en el Ministerio de Defensa se estructura en cinco áreas: «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en poder de las empresas», «Seguridad de la Información en las Instalaciones» y «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones». Obviamente, este quinto capítulo se centrará en esta última área, aunque como es lógico tiene una estrecha relación con el resto de áreas.

En el año 2005 el Ministerio de Defensa vio la necesidad de afrontar un proceso de modernización, consecuencia de la evolución de las tecnologías de la información, que recogiera su política de seguridad de la información como documento único del cual debería emanar toda norma interna en materia de seguridad de la información del Ministerio, facilitando así, la necesaria coordinación en el desarrollo normativo posterior y de este modo alcanzar un conjunto normativo equilibrado, completo y con criterios unificados.

En el año 2006, se publicó la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprobó la mencionada política de seguridad de la información, con objeto de alcanzar la protección adecuada, proporcionada y razonable de la Información del Ministerio de Defensa, mediante la preservación de sus requisitos básicos de seguridad: confidencialidad, integridad y disponibilidad.

Esta OM derogó la Orden Ministerial Comunicada 1/1982, de 25 de enero, por la que se aprobaban las normas para la protección de la documentación y material clasificado, y la Orden Ministerial 76/2002, de 18 de abril, por la que se aprobaba la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o

transmitida por sistemas de información y telecomunicaciones, si bien esta última estará transitoriamente en vigor en tanto no se publiquen las normas de «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», y «Seguridad de la Información en las Instalaciones», correspondientes al desarrollo normativo de segundo nivel de la política de seguridad de información del Ministerio. Su finalidad era establecer la estructura y responsabilidades en materia INFOSEC en el Ministerio de Defensa.

En la OM 76/2002, continúa estando por tanto en vigor lo siguiente:

- Que el Ministro de Defensa es la «Autoridad de Acreditación de la Seguridad de los Sistemas», si bien estará asistido por las siguientes «Autoridades Delegadas de Acreditación» (ADA):
  a) El Jefe del Estado Mayor de la Defensa, que es la ADA en los Sistemas conjuntos de Mando y Control, Inteligencia, Telecomunicaciones y Guerra Electrónica. El JEMAD cuenta con un Organismo de Acreditación para apoyo a sus funciones, que se ha articulado a través de la DIVICS (División CIS) y su Sección de Seguridad de la Información CIS.
  b) El Subsecretario de Defensa (SUBDEF), que es la ADA en el ámbito de los Sistemas responsabilidad del Órgano Central y periféricos del Ministerio de Defensa.
  c) El Jefe de Estado Mayor del Ejército de Tierra, el de la Armada y el del Ejército del Aire, que son las ADA,s en los Sistemas específicos de sus respectivos Ejércitos.
  d) El Director del CNI, que es la ADA en los Sistemas responsabilidad de su Organismo y en el ámbito internacional (OTAN, UEO y otras organizaciones internacionales). Asimismo es responsable de asesorar al resto de las ADA,s en materia INFOSEC (32) y coordinar en materia Criptográfica y TEMPEST(33). Designará un Organismo de Acreditación para apoyo a sus funciones.

También recoge esta OM la definición de acreditación de sistemas CIS, que creo pertinente traer a colación. En el ámbito de la seguridad de la in-

(32) Protección de la información almacenada procesada o transmitida, por Sistemas de Información y Telecomunicaciones (Sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios Sistemas.

(33) Transient Electro Magnetic Pulse Emanation Standard.

formación CIS, se entiende por «acreditación», la autorización otorgada a un Sistema por la Autoridad de Acreditación, para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación. La acreditación siempre estará basada en la Declaración de Requisitos Específicos de Seguridad del Sistema (DRES) y en los Procedimientos Operativos de Seguridad (POS), aparte de ser necesario un análisis de riesgos y un concepto de operación para la obtención de la citada autorización.

Volviendo de nuevo a la OM 76/2006, se establecen en dicha política las definiciones, los conceptos y los principios básicos comunes a todos los ámbitos del Departamento. Se designa como Director de Seguridad de la Información del Ministerio al Secretario de Estado de Defensa, y se le encomienda, en el ámbito del departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas.

Se establece, asimismo, el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa, como órgano de coordinación de la seguridad de la información del Ministerio, que preside el Secretario de Estado de Defensa.

En el año 2010 se ha publicado la Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa. Estas normas tienen por finalidad establecer la estructura funcional de la Seguridad de la Información del Ministerio de Defensa, sus responsables y cometidos.

En ella, se designa al Director General de Infraestructura como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones y en las instalaciones. En el ejercicio de los citados cometidos será el interlocutor, a nivel corporativo, del Ministerio de Defensa con el Centro Nacional de Inteligencia y organismos externos al Departamento, con facultad de representar al Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF) en el ámbito de sus competencias.

Asimismo, se designa a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de De-

fensa (Inspección General CIS) como órgano de apoyo técnico para la realización de las tareas encomendadas al Director General de Infraestructura en las áreas de su respectiva competencia. No obstante, parece estarse preparando una reorganización de esta Inspección que podría afectar a su dependencia orgánica y funciones.

Por otra parte, se designa al Director General de Armamento y Material como responsable del área de seguridad de la información en poder de las empresas. En el ejercicio de los citados cometidos será el interlocutor, a nivel corporativo, del Ministerio de Defensa con el Centro Nacional de Inteligencia y organismos externos al Departamento, con facultad de representar al DSIDEF en el área de su competencia.

Para llevar a cabo la dirección, ejecución y supervisión de la Seguridad de la Información del Ministerio de Defensa se establecen dos niveles funcionales: el Nivel Corporativo y el Nivel Específico.

El Nivel Corporativo, bajo la autoridad del DSIDEF, es responsable, en el ámbito del Departamento, de la dirección, coordinación, evaluación y supervisión de las medidas de seguridad de la información en las cinco áreas ya citadas.

En el Nivel Específico se establecen siete ámbitos (EMAD, los tres CCGG, SEDEF, SUBDEF y UME). El jefe o autoridad de cada uno de estos ámbitos, es el máximo responsable de la dirección, coordinación, ejecución y supervisión de las medidas de seguridad de la información específicas de cada ámbito, siguiendo los criterios unificados establecidos en el Nivel Corporativo. El Jefe de Estado Mayor de la Defensa, ejerce además las que son de su competencia respecto de los sistemas conjuntos de Mando y Control, Inteligencia, Telecomunicaciones y Guerra Electrónica.

La necesaria coordinación entre los niveles funcionales y sus diferentes ámbitos se realiza a través del ya mencionado Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa que se reunió por primera vez en septiembre de 2010. El seguimiento de las directrices establecidas en la Política de Seguridad de la Información del Ministerio de Defensa es realizado por el Comité de Seguimiento de la Seguridad de la Información del Ministerio de Defensa, que todavía no se ha reunido.

Asimismo, se establece que la Dirección General de Infraestructura es el órgano directivo al que corresponde, entre otras cosas, la prepara-

ción, planeamiento y desarrollo de los sistemas, tecnologías y **políticas de seguridad de la información del departamento**, así como la supervisión y dirección de su ejecución.

De la Dirección General de Infraestructura dependen directamente, entre otros, los siguientes órganos directivos relacionados con la seguridad de la información CIS:

- El Laboratorio de Ingenieros del Ejército, que entre otras tareas es el encargado de las imprescindibles mediciones «zoning» (34) de los locales en los que se instalan sistemas TIC. Estas mediciones también son realizadas por el GRUTRA del EA y por el CCN.
- La Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones, que ejercerá las funciones de definición de las políticas y estrategias corporativas en el ámbito de la Administración Electrónica, las tecnologías de la información, telecomunicaciones y seguridad de la información del Ministerio de Defensa, así como la planificación y coordinación de las actuaciones en estas materias.

En cuanto a la organización de la ciberseguridad en el Estado Mayor de la Defensa (EMAD), esta está regulada mediante la Instrucción 40/2008, de 15 de abril, del Jefe de Estado Mayor de la Defensa. En ella, se establece que la División de Sistemas de Información y Telecomunicaciones (DIVCIS) es el órgano del EMACON responsable del planeamiento, dirección y control del Sistema de Mando y Control Militar de las Fuerzas Armadas (SMCM), y de los sistemas de información y las telecomunicaciones que lo soportan. Son funciones concretas de la DIVCIS, entre otras, el planear, dirigir y coordinar las actividades **en materia de seguridad de la información en los sistemas de información y telecomunicaciones** que sean competencia del JEMAD. Para ello, se sirve de la Sección de Seguridad de la Información CIS, que es responsable de planear, coordinar y, en su caso, ejecutar, las actividades en materia de seguridad de la información en los sistemas de información y telecomunicaciones que sean responsabilidad del JEMAD, así como de la coordinación con los Ejércitos en dicho campo.

(34) Estas mediciones se efectúan para determinar el grado de protección ante emanaciones electrónicas e inducciones indeseables de los equipos a instalar y que pueden provocar pérdida o fugas de información de forma involuntaria, o su obtención intencionada por individuos malintencionados dotados de la tecnología adecuada. Este problema es especialmente importante en instalaciones que se encuentren en el interior de ciudades y que no cuenten con un perímetro de seguridad adecuado.

Dentro de este apartado normativo referente a la seguridad de la información en los sistemas CIS, no podríamos dejar de mencionar al Centro Nacional de Inteligencia (CNI), pues aparte de que en el Real Decreto 1126/2008 (ya mencionado anteriormente) por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, dispone que está adscrito orgánicamente al Ministerio de Defensa, con dependencia directa del Ministro, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional asigna a éste una serie de funciones que inciden directamente en todas las actuaciones de seguridad de la información del Ministerio. En él, se atribuye al Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), la responsabilidad de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, además de garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica. Asimismo, es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones.

INFRAESTRUCTURA. ÁMBITOS DE PROPÓSITO GENERAL Y MANDO Y CONTROL

Plan Director CIS

La seguridad de la información CIS en el Departamento tiene dos ámbitos de muy diferentes objetivos y características: la WAN (35) de Mando y Control y la de Propósito General, de acuerdo con la Orden DEF/315/2002, de 14 de febrero, que aprobó el Plan Director de Sistemas de Información y Telecomunicaciones (PDCIS). Para su dirección, gestión y seguimiento, se creó el Comisionado del Plan, que luego pasó

(35) Las **Redes de área amplia** (WAN) son redes informáticas que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (hosts). Estos están conectados por la red que lleva los mensajes de un host a otro. Estas LAN de host acceden a la subred de la WAN por un encaminador o router. Suelen ser por tanto redes punto a punto.

a denominarse Inspección General CIS. En el PDCIS, se establecía que la Plataforma Informática y la Arquitectura técnica del Ministerio evolucionarían hacia un escenario cuya principal característica era la existencia de dos únicas Redes de Área Extensa (WAN) para dar soporte a todos los Sistemas de Información del Ministerio:

- Una WAN para Mando y Control Militar, cuyo despliegue y extensión se correspondería con el de los Puestos de Mando y los Centros de Comunicación. Esta WAN, se debería interconectar con los entornos tácticos, con los similares de la OTAN y con las redes de sensores que fuera necesario. Desde el punto de vista de la seguridad, al ser su orientación de carácter eminentemente clasificado y de utilización para operaciones y planeamiento militar, los sistemas que la componen deben estar acreditados al nivel de clasificación adecuado, normalmente RESERVADO Y NATO/UE SECRET, lo que como se puede imaginar supone unos condicionantes de administración, establecimiento de medidas de seguridad, cifrado y arquitectura muy exigentes y complejas.
- Una WAN Corporativa de Propósito General (PG), que daría soporte a todos los sistemas de información que no fueran específicos para mando y control y se extendería a todos los emplazamientos. Este entorno incluía la conexión a Internet del Ministerio de Defensa, a través de un único punto de acceso común para todos los usuarios y sería la única que la WAN de Propósito General tendría con el exterior. La WAN PG se configura y explota con una perspectiva corporativa e integrada, para lo que se creó el CCEA. En este único Centro Corporativo de Explotación y Apoyo se concentraron los entonces existentes Centros de Proceso de Datos y Explotación, ubicados en dos emplazamientos distintos.

Respecto de las Redes de Área Local (LAN), con carácter general, los emplazamientos del Ministerio disponen de una LAN integrada en la WAN de Propósito General. Además, en aquellos emplazamientos que lo requieren, se han establecido LANs para Mando y Control, físicamente aislada de la anterior e integrada en su correspondiente WAN. Por último, en aquellos emplazamientos que incluyen un Centro de Elaboración de Inteligencia puede existir una tercera LAN conectada también a la WAN para Mando y Control. Además y mientras que no se llegue a la implantación del concepto NEC, ya citado anteriormente, es necesario mantener una serie de extensiones de redes clasificadas de diferentes organizaciones, como la NATO Secret WAN, la ESPDNET de la UE, etc.

En cuanto a la interoperabilidad, existe una única plataforma tecnológica de interoperabilidad básica (mensajería interpersonal, flujos de trabajo, herramientas de trabajo en grupo, etc.) con dos dominios diferenciados para cada una de las dos redes WAN. Los servicios de directorio están basados en un modelo de dos directorios (uno por WAN), soportados en una única herramienta, con un diseño de arquitectura tal que permite en el futuro integrar fácilmente ambas estructuras, para lograr un único directorio.

En lo referente a Instrumentos y herramientas de seguridad, se ha desarrollado una infraestructura de Clave Pública (PKI) como soporte de seguridad para el acceso a la plataforma y a los sistemas de información, para el cifrado y para la firma electrónica. Para ello, se ha constituido una única Autoridad de Certificación (CA) raíz, para la gestión de dicha infraestructura con dos CA,s delegadas, una para cada entorno WAN, y tantas Agencias de Registro (RA) como sean necesarias. Como soporte físico de los certificados se decidió utilizar tarjetas con chips individuales y personalizadas para cada usuario del Ministerio. Todavía no se ha terminado de desplegar para la WAN PG y en la WAN de Mando y Control se empezará su despliegue en breve, aunque se ha elegido un soporte USB con el correspondiente chip.

COOPERACIÓN INTERNACIONAL

España es «Sponsoring Nation» del CCD COE («Cooperative Cyberdefence Center Of Excellence») de Tallin (Estonia) desde el mes de mayo de 2008. Como tal, tiene un representante en el «Steering Committee» para la definición de los POWs («Program Of Work») y dirección y control de sus actividades. Además, tiene desde su participación dos miembros en su plantilla, un Teniente Coronel en la vacante de Jefe del Departamento de Doctrina y Adiestramiento y un civil en calidad de científico en el Departamento de Investigación y Desarrollo. Estas personas dependen funcionalmente del EMAD, a través del Jefe de la Sección de Seguridad de la Información CIS.

Este Centro está realizando una considerable actividad promoviendo cursos de alto nivel técnico, conferencias internacionales con expertos de todo el mundo, acuerdos con diferentes instituciones y organismos, que no solo abarcan los aspectos tecnológicos sino también las consideraciones legales correspondientes a las actuaciones en el ciberespacio,

para lo que cuenta con un embrión de un Departamento a este respecto, que en breve obtendrá su dotación adecuada de recursos.

En este apartado hay que destacar también los trabajos y acuerdos internacionales que en el ministerio se han llevado a cabo o se encuentran en proceso de realización, tanto para el intercambio de información de ciberdefensa como para la adquisición de diversos equipos de cifrado o de gestión y distribución electrónica de claves para los cifradores. Es necesario nombrar asimismo, los trabajos en curso para el desarrollo de redes de coalición mediante federación de las diferentes extensiones nacionales, como es el caso de la AMN con la red de misión de ISAF, que conlleva un esfuerzo considerable desde el punto de vista de la seguridad. Mención aparte merece la participación en ejercicios de carácter multinacional en el ámbito de la ciberdefensa, que serán detallados en el siguiente apartado.

No se puede olvidar que también existe un amplio número de simposios, cursos internacionales (en las escuelas de la Latina y Oberammergau), grupos de trabajo, subcomités como el SC «information assurance» de la Alianza Atlántica, «workshops» como el de ciberdefensa OTAN, etc, en los que se viene trabajando desde hace años y que contribuyen a mejorar el conocimiento de nuestro personal y la interoperabilidad y eficacia de nuestros sistemas CIS, dotándoles de la seguridad adecuada. Cabe destacar dentro de este apartado la cumbre de Directores de Seguridad de la Información CIS de países de la OTAN, de reciente andadura (lleva celebrándose dos años) y en la que se tratan a alto nivel el estado, retos y problemas de la seguridad de los sistemas CIS OTAN y en especial la problemática relacionada con los de mando y control desplegados en operaciones.

FORMACIÓN Y ADIESTRAMIENTO

Sensibilización, Concienciación y Formación

La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio. La seguridad CIS es un campo amplísimo, que requiere de una especialización muy considerable y que además exige que dentro de ella se contemplen a la vez diversos campos de especialización. Es muy difícil encontrar personas que dominen todos estos campos. Por intentar identificarlos, podríamos decir que serían: la electrónica de red y comunicaciones (switches, routers, cifradores, etc),

los sistemas operativos y aplicaciones, las bases de datos y las aplicaciones web. Evidentemente no es lo mismo el conocimiento que debe tener un administrador de seguridad de una red que las personas que componen un equipo de acreditación de sistemas o las que pertenecen a un equipo de respuesta ante incidentes o de un CERT, lo que a su vez nos da idea de diferentes escalones y diferentes requerimientos. Como podemos imaginarnos, la formación mencionada requiere, además, de una continua actualización acorde con la vertiginosa evolución de las tecnologías de la información.

A modo de ejemplo de lo mencionado en el párrafo anterior, el reconocido Instituto SANS(36), ha sido patrocinador de una compañía que ha realizado un reciente estudio sobre la necesidad de profesionales de seguridad en el Reino Unido, llevado a cabo mediante encuesta entre los profesionales del sector más destacados y experimentados. Los principales resultados han sido que el Reino Unido tiene dificultad en encontrar personal para trabajos de ciberseguridad (aproximadamente el 90% de los encuestados) y los profesionales piensan que el número de puestos de trabajo necesarios se incrementará (60 % de las respuestas) a la vez que han detectado una disminución de solicitantes de puestos de trabajo en el conjunto del sector de Tecnologías de la Información. En cuanto a las razones que llevan a los profesionales de la seguridad a disfrutar de su trabajo, se destacan el hecho de que «no hay dos días iguales», el desafío continuo y lo interesante del trabajo y la sensación de que se está realizando algo que es realmente útil.

En el ámbito militar, la política de personal no favorece esta puesta al día, ya que hay que conjugar ésta con los cambios de destino, el cumplimiento de condiciones para dar perspectivas de promoción, los cursos de capacitación para el ascenso, etc. Todo ello lleva a la necesidad de contar con personal contratado de empresas, pero a la vez teniendo en cuenta que precisamente la seguridad es la menos externalizable en el caso de nuestras FAS, del gran coste económico que esto supone y por último en nuestros días con el problema añadido de la crisis económica que está ralentizando y en algunos casos impidiendo que se puedan desarrollar conforme a las previsiones y necesidades diversos programas de seguridad CIS.

No obstante, en este campo se pueden citar un elevado número de iniciativas, que van desde charlas rutinarias de concienciación para el

(36) www.sans.org/

personal que se incorpora a nuevos destinos, a cursos online, seminarios, cursos en los programas de formación y perfeccionamiento de los tres ejércitos, cursos conjuntos, «máster» por diferentes universidades subvencionados por el Ministerio o jornadas técnicas de temas específicos. Además, todos los años se celebran unas jornadas en el CESEDEN, denominadas Jornadas de Seguridad de la Información del MINISDEF. Estas se organizan en colaboración entre el EMACON (Estado Mayor Conjunto) y la DIGENIN (Dirección General de Infraestructuras), para concienciar y sensibilizar en esta materia y en su última edición supuso un gran éxito de asistencia con más de 350 participantes.

Ejercicios de ciberdefensa

El EMACON viene participando activamente desde el año 2008 en diversos ejercicios de ciberdefensa internacionales, entre los que se pueden citar los tres últimos ejercicios organizados por EEUU («US DoD International Cyber Defense Workshop») y los dos primeros ejercicios de ciberdefensa OTAN, en noviembre de 2009 y de 2010. Los ejercicios de EEUU han sido patrocinados por la «Office of the Secretary of Defense Networks and Information Integration, International Information Assurance Program (IIAP)» y dirigido por la «University of Nebraska Omaha». Por parte del EMAD participaron miembros de la Sección de Seguridad de la Información formando equipos con miembros invitados de dos CERTs nacionales: el CCN-CERT(37) e IRIS-CERT(38). La participación se llevó a cabo de manera remota a través de Internet. En cuanto al ejercicio OTAN de 2009, se pretendía comprobar los procedimientos entre el CERT OTAN y los CERT gubernamentales de los países participantes.

Durante 2009 y 2010, se ha participado en los trabajos del EUMS (European Union Military Staff) para la definición del Concepto de CNOs («Computer Network Operations») en operaciones militares lideradas por la UE.

Ya a nivel nacional, en octubre de 2009, el EMACON, a través de la Sección de Seguridad de la Información CIS y con la colaboración de Isdefe, organizó el Primer Ejercicio de Ciberdefensa de las FAS (ECD09), con más de 80 participantes de 20 equipos pertenecientes al Ejército de Tierra, Armada, Ejército del Aire, Cuartel General del Estado Mayor de la

(37) www.ccn-cert.cni.es/
(38) www.rediris.es/servicios/iris-cert/

Defensa (EMAD), Centro de Inteligencia de las Fuerzas Armadas (CIFAS), Centro Criptológico Nacional (CCN) y Guardia Civil.

Los resultados del ejercicio permitieron conocer con más detalle las capacidades técnicas actuales existentes en el Ministerio de Defensa en este ámbito de la Ciberdefensa, así como una primera aproximación de los diferentes centros y unidades con recursos humanos y conocimiento en esta área. Se ha podido confirmar que existe una capacidad inicial y que es vital continuar potenciando estas iniciativas para adecuarnos a las amenazas actuales, que están en continuo cambio. Es de destacar que la valoración realizada por los participantes, fue muy positiva.

En este mes de octubre se va a realizar el Segundo Ejercicio de ciberdefensa de las FAS. Para esta ocasión, la demanda de participación ha crecido de manera considerable, lo que constituye una excelente noticia. En esta edición, el ejercicio se dirigirá y controlará por entero desde el EMAD y se han introducido dos importantes mejoras en los escenarios de defensa y ataque, incluyendo sistemas SCADA y herramientas de análisis y correlación de eventos.

CIFRA

Como ya se ha citado anteriormente, corresponde al CCN la responsabilidad de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, además de informar sobre la adquisición coordinada del material criptológico, formar al personal de la Administración especialista en este campo y certificar la seguridad de las tecnologías criptológicas. La cifra es un aspecto imprescindible de la seguridad de nuestras comunicaciones. El uso masivo de las tecnologías de la información requiere de equipamiento de cifra acorde con las necesidades de los usuarios. Toda información clasificada que haya de ser enviada fuera del nodo donde se ha creado ha de estar cifrada. La certificación del cifrador (métrica de su capacidad) y algoritmos empleados deben estar de acuerdo con el nivel de clasificación de la información, si bien, en redes como pueda ser la WAN de Mando y Control, se utilizan los de más alta protección para ahorro de medios. Disponer de criptología nacional con seguridad verificable es un principio irrenunciable, ya que poner nuestras comunicaciones en manos de cifradores y algoritmos desconocidos o no controlados en todo su proceso de fabricación es inaceptable.

Las tendencias de las nuevas generaciones de equipos de cifra apuntan a contar con las siguientes características fundamentales: interoperabilidad entre cifradores con diferentes redes de acceso, interoperabilidad a nivel nacional y con aliados (mediante la implementación de protocolos de interoperabilidad como SCIP) y certificación múltiple (Nacional, OTAN, UE, mediante el empleo de un único equipo para proteger información diversos orígenes); asimismo, la implementación de módulos reprogramables es una característica de gran utilidad, especialmente de cara a las operaciones en coalición, que demandan la cesión temporal de medios de cifra a países con los que no existen los necesarios acuerdos o marcos de confianza en este campo.

Por otra parte, el mercado de productos de cifra es reducido, limitado casi exclusivamente a la Administración General del Estado (Presidencia del Gobierno, Ministerios de Asuntos Exteriores y su principal cliente, el Ministerio de Defensa). Existen pocas empresas nacionales que desarrollan productos cripto, que además son de tamaño y facturación reducido. A la debilidad del sector fabricante hay que añadir la rápida evolución de las tecnologías de la información que obligan a que el esfuerzo de financiación del desarrollo sea sostenido en el tiempo, para poder abordar la fabricación de nuevos productos de cifra que satisfagan las necesidades del Ministerio de Defensa.

CONCLUSIONES

Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera. En menos de una generación, las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico.

Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar y aire, a través del ciberespacio. La situación podría agravarse con la actual crisis económica, ya que ésta está implicando una restricción en inversiones de seguridad tanto en empresas como en las administraciones públicas y las FAS.

La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias.

En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes.

La ciberguerra es asimétrica. El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares. Muchos ejércitos están desarrollando capacidades ofensivas en el ciberespacio y se estima que más de 100 servicios de inteligencia extranjeros llevan a cabo estas actividades.

Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados; tanto su software como su hardware pueden ser saboteados antes de ser unidos en un sistema en explotación. El riesgo de manipulación en el proceso de fabricación es totalmente real y es la menos comprendida de las ciberamenazas. El sabotaje es prácticamente imposible de detectar y peor todavía de erradicar.

Ejércitos de diversos países han reconocido formalmente al ciberespacio como un nuevo dominio de enfrentamiento («Global Commons»). Aunque el ciberespacio es un dominio hecho por el hombre, se ha hecho tan crítico para las operaciones militares como la tierra, el mar, el aire y el espacio.

La convergencia a NEC exigirá una mayor interconexión con otros sistemas (Federación de Redes), incluso con ONGs, lo que exigirá un considerable esfuerzo en seguridad de la información.

A nivel nacional, el Ministerio de Defensa ha llevado a cabo numerosas iniciativas, publicando la Política de Seguridad de la Información, sus normas de aplicación y tomando un buen número de medidas para incrementar la seguridad de su información, tanto en el ámbito de la red de Propósito General como en el de Mando y Control.

La seguridad de la información en el Ministerio de Defensa se estructura en cinco áreas: «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en poder de las empresas», «Seguridad de la Información en las Instalaciones» y «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», designándose Director de Seguridad de la Información del Ministerio al Secretario de Estado de Defensa, y asignándole, en el ámbito del departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas. También se designa al Director General de Infraestructura como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones y en las instalaciones y como órgano de apoyo técnico para la realización de estas tareas, se designa a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa (Inspección General CIS); como órgano de coordinación de la seguridad de la información del Ministerio, se establece, el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa.

La dirección, ejecución y supervisión de la Seguridad de la Información del Ministerio de Defensa se lleva a cabo en dos niveles funcionales: el Nivel Corporativo y el Nivel Específico. El Nivel Corporativo, bajo la autoridad del DSIDEF y el Nivel Específico en siete ámbitos (EMAD, los tres CCGG, SEDEF, SUBDEF y UME), siendo el jefe o autoridad de cada uno de estos ámbitos, el máximo responsable de la dirección, coordinación, ejecución y supervisión de las medidas de seguridad de la información específicas de cada ámbito, siguiendo los criterios unificados establecidos en el Nivel Corporativo. El Jefe de Estado Mayor de la Defensa, ejerce además las que son de su competencia respecto de los sistemas conjuntos de Mando y Control, Inteligencia, Telecomunicaciones y Guerra Electrónica.

El Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), se le asigna la responsabilidad de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, además de garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

En el ámbito de la cooperación internacional en la ciberdefensa, España es «Sponsoring Nation» del CCD COE («Cooperative Cyberdefence Center Of Excellence») de Tallin (Estonia) y ha participado en los trabajos del EUMS para la definición del Concepto de CNOs en operaciones militares lideradas por la UE; además, el EMAD participa en un amplio número de simposios, cursos internacionales, grupos de trabajo, «workshops» y subcomités OTAN, etc, sin olvidar que el EMACON viene participando activamente desde el año 2008 en diversos ejercicios de ciberdefensa internacionales y organizando uno anual para las FAS.

La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio. La seguridad CIS es un campo amplísimo, que requiere de una especialización muy considerable y que además exige que dentro de ella se contemplen a la vez diversos campos de especialización. Dentro de la formación y el adiestramiento y a nivel nacional, el EMACON, ha organizado dos Ejercicios de Ciberdefensa de las FAS con alrededor de 100 participantes distribuidos en 25 equipos pertenecientes al Ejército de Tierra, Armada, Ejército del Aire, Cuartel General del Estado Mayor de la Defensa (EMAD), Centro de Inteligencia de las Fuerzas Armadas (CIFAS), Centro Criptológico Nacional (CCN) y Guardia Civil, que está contribuyendo a la creación de una comunidad de ciberdefensa en el Ministerio.

La cifra es un aspecto imprescindible de la seguridad de nuestras comunicaciones. El uso masivo de las tecnologías de la información requiere de equipamiento de cifra acorde con las necesidades de los usuarios. Disponer de criptología nacional con seguridad verificable es un principio irrenunciable, ya que poner nuestras comunicaciones en manos de cifradores y algoritmos desconocidos o no controlados en todo su proceso de fabricación es inaceptable.

Las tendencias de las nuevas generaciones de equipos de cifra son: interoperabilidad entre cifradores con diferentes redes acceso, interoperabilidad a nivel nacional y con aliados, módulos reprogramables y certificación múltiple.

El mercado de productos de cifra es reducido, limitado casi exclusivamente a la Administración General del Estado. Existen pocas empresas nacionales que desarrollen productos cripto, que además son de tamaño y facturación pequeñas. A la debilidad del sector fabricante hay que añadir la rápida evolución de las tecnologías de la información que obligan a que el esfuerzo de financiación del desarrollo sea sostenido en el tiempo.

BIBLIOGRAFÍA

1. TIKK, Eneken; KASKA, Kadri; VIHUL, Liis;. *International Cyber Incidents, Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.
2. CZOSSECK, Christian; GEERS, Kenneth;. «The Virtual Battlefield: Perspectives on Cyber Warfare.» Tallinn: IOS Press BV, 2009.
3. LYNN, William J. III (Deputy Defense Secretary), *Defending a New Domain, The Pentagon's Cyberstrategy, Council on Foreign Relations, September/October 2010.*
4. KREKEL Byan, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* Northrop Gruman Corporation.
5. *SHARMA Amit, Cyber Wars: A Paradigm Shift from Means to Ends,* Institute for System Studies and Analysis del Ministerio de Defensa de la India.
6. PASTOR ACOSTA, Oscar; PEREZ RODRÍGUEZ, José Antonio; ARNÁIZ DE LA TORRE, Daniel; TABOSO BALLESTEROS, Pedro;. *Seguridad Nacional y Ciberdefensa.* Madrid: Cátedra ISDEFE-UPM, 2009.
7. *Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación* de la Política de Seguridad de la Información del Ministerio de Defensa.
8. Real Decreto 1126/2008, de 4 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa.
9. Instrucción 40/2008, de 15 de abril, del Jefe de Estado Mayor de la Defensa, sobre organización del Estado Mayor de la Defensa.
10. Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa.
11. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
12. Orden Ministerial número 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones.

13. Orden DEF/315/2002, de 14 de febrero, por la que se aprueba el Plan Director de Sistemas de Información y Telecomunicaciones y se establece, para su dirección, gestión y seguimiento, el Comisionado del Plan.

14. Informe de Amenazas CCN-CERT IA-01/09. Ciberamenazas 2009 y Tendencias 2010. Centro Criptológico Nacional.

15. Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations. The Secretary of Defense, EE.UU. JUN 09.

16. Computer Network Defense Roadmap. Department of the Navy. Chief Information Officer. May 09.

17. La ciberofensiva de China (y cómo pueden responder los EE.UU). DEF/361/09. Agregaduría de Defensa. 03 NOV 09.

18. Multiple Futures Project. Final Report. April 2009.

19. Virtual Criminology Report 2009. McAfee.

20. NATO Cyberdefence concept. Feb 09.

21. Directiva de Defensa Nacional 1/2008.

22. Concepto de Estrategia Militar.

23. Resolución A/63/37 de la Asamblea General de Naciones Unidas. 09 ENE 09.

24. Serie CCN-STIC (https://www.ccn-cert.cni.es/)

25. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

26. Normativa y Orientaciones (http://www.cni.es/es/ons/documentacion/normativa/).
    - NORMA NS/01: Infraestructura Nacional de Protección de la Información Clasificada.
    - NORMA NS/02: Seguridad en el personal. Habilitación de seguridad del personal.
    - NORMA NS/03: Seguridad Física.
    - NORMA NS/04: Seguridad de la Información.
    - NORMA NS/05: Seguridad en los Sistemas de Información y Comunicaciones.

- NORMA NS/06: Seguridad Industrial.
- NORMA NS/08: Protección de la Información Clasificada OTAN manejada en Sistemas de Información y Comunicaciones (CIS).
- Orientaciones:
  - Seguridad Documental:
    * OR-ASIP-04-01.03 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.
  - Seguridad en el Personal:
    * OR-ASIP-02-01.01 – Confección Solicitud HPS.
    * OR-ASIP-02-02.02 – Instrucción de Seguridad del Personal para acceso a IC.pdf.
  - Seguridad Física:
    * OR-ASIP-01-01.02 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.
    * OR-ASIP-01-02.02 – Orientaciones para la Constitución de Zonas de Acceso Restringido.

CAPÍTULO SEXTO

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD. CIBERTERRORISMO

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD. CIBERTERRORISMO

POR JAVIER CANDAU ROMERO

RESUMEN

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Todas las naciones de nuestro entorno están desarrollando iniciativas para intentar controlar las amenazas que vienen del ciberespacio. La mayoría de ellas está apostando por concentrar y fortalecer las capacidades técnicas y de coordinación actuando especialmente sobre la respuesta a incidentes de seguridad. Se analizan las estrategias nacionales más relevantes.

En España las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos que abordan el problema de forma parcial. Es necesario por tanto impulsar actuaciones en este sentido fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante este tipo de amenazas. La dotación presupuestaria se considera crítica si se quieren llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la amenaza. La aproximación debe ser a todos los niveles; el sector público, la industria, los ciudadanos y los aliados internacionales.

Palabras clave: Seguridad, ciberespacio, tecnologías, información, comunicaciones, amenaza, estrategia nacional, ataques, redes, internet, ciberseguridad, ciberataque, ciberdefensa, ciberterrorismo, ciberespionaje incidente, infraestructura crítica, SCADA.

NATIONAL CYBERSECURITY STRATEGIES. CYBERTERRORISM

ABSTRACT

Cyberattacks are very profitable in terms of the efforts needed for their performance, the risks assumed and the political or economic profits that might be achieved, and they affect transversely both the public and private sectors, as well as the citizens. All neighbouring nations are developing initiatives to try to monitor the threats coming from the cyberspace. Most of them are placing particular emphasis on focussing on and strengthening the coordination and technical capabilities, acting particularly on the response to security incidents. The most outstanding national strategies are analysed.

In Spain, cyberspace liabilities are highly compartmentalized among different bodies that tackle the problem partially. Thus, it is necessary to foster actions in this sense by strengthening the response capabilities in case of incident and the intelligence capabilities vis-à-vis this kind of threats. The budget allocation is considered critical to follow the lines of action presented as possible solutions to reduce the threat. Involvement should be made at all levels: public sector, industry, citizens and international allies.

Key words: Security, cyberspace, technology, information, communications, threats, national strategy, attacks, networks, Internet, cyber security, cyber attack, cyber defense, cyber terrorism, cyber espionage, incident, critical infrastructure, SCADA.

INTRODUCCIÓN

En los últimos años se ha detectado un incremento constante de vulnerabilidades y amenazas sobre los sistemas y tecnologías de la información y comunicaciones. Estas amenazas, que no tienen por qué ser deliberadas (los errores y omisiones del personal autorizado y bienintencionado pero desconocedor de buenas prácticas de seguridad también lo son), evolucionan continuamente y representan un verdadero desafío para los responsables de proporcionar servicios electrónicos.

En el caso de las amenazas voluntarias, el reto es aún mayor si tenemos en cuenta que aquellos que intentan infiltrarse o explotar nuestros

sistemas emplean recursos mejores y más sofisticados. Además, en la actualidad los ataques se pueden llevar a cabo desde cualquier parte del mundo y, en muchos casos, las posibilidades de descubrir su origen, e incluso su presencia, son muy remotas por lo que es necesario un esfuerzo de todos para intentar abordar este problema.

Con el desarrollo de las tecnologías de comunicaciones, se ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios han eliminado las barreras de distancia y tiempo. En el nuevo espacio relacional –el ciberespacio–, se han diluido las fronteras nacionales y, a la vez, se ha producido un considerable aumento de las posibilidades pero también de las amenazas, acrecentadas éstas por el constante crecimiento de la dependencia cibernética de las sociedades avanzadas.

Este hecho se agrava con la excesiva uniformidad de los medios empleados (tcp/ip, Windows, Web...) que facilitan la rentabilidad de la formación de los atacantes y el impacto global de la explotación de las vulnerabilidades y los fallos detectados. En definitiva la superficie de ataque es inmensa.

Por ello, ningún sistema, incluidos todos los de la Administración, está a salvo de sufrir un ataque de graves consecuencias como el robo, pérdida, destrucción o extracción de dispositivos de almacenamiento; destrucción o modificación de datos almacenados; redirección de Información para usos fraudulentos; interceptación de datos mientras se procesan, correo no deseado, etc.

Los ciberataques normalmente comparten las siguientes características comunes:

– **Bajo coste**. Muchas herramientas de ataque se pueden descargar de forma gratuita o con un coste muy bajo para el daño que pueden causar.
– **Fácil empleo**. Para muchos ataques no son necesarios grandes conocimientos técnicos. Existen herramientas con unos interfaces de usuario muy amigables y sencillas de usar.
– **Efectividad.** Existe una probabilidad muy alta de alcanzar los objetivos buscados con estos ataques por la ausencia de políticas de empleo o la limitación de recursos existentes en la parte defensiva debido a la falta de concienciación de las organizaciones gubernamentales, empresas y ciudadanos.
– **Bajo Riesgo para el atacante**. Es muy difícil atribuir un ataque con las herramientas de ocultación del origen existentes actualmente

en INTERNET y por la diferencia de legislaciones de los diferentes países.

Además, algunos de los siguientes factores tecnológicos incrementan la posibilidad de estos ataques:

– La complejidad creciente de la tecnología hace más difícil determinar el grado de seguridad de un determinado producto o sistema.
– La rapidez de la evolución tecnológica y las exigencias y competitividad del mercado ocasionan que, con frecuencia, se desplieguen productos con vulnerabilidades y fallos de seguridad que son aprovechados por los agresores.
– Existe un mayor riesgo en el caso de productos fabricados en países fuera de la órbita occidental, ya que es más difícil controlar la introducción de elementos inseguros.
– Hay una relativa falta de madurez de la industria de las tecnologías de la información y las comunicaciones, al no considerar la seguridad como un factor de diseño de los productos o sistemas.
– Se constata un constante incremento de la interconexión de todo tipo de sistemas utilizando Internet.

Existen evidencias de que determinados países tienen programas de capacitación técnica para lograr realizar ciberataques. En algunos casos, dicha capacitación técnica es considerada y abordada como una capacidad militar más con la que se plantean lograr la superioridad.

En un primer análisis sobre la situación global de la cibercriminalidad, puede afirmarse que las técnicas utilizadas son cada vez más depuradas y que existe una mayor interrelación entre los ciberdelincuentes de diversos países.

Muchos países han desarrollado o están desarrollando estrategias nacionales de Ciberdefensa con las que persiguen conseguir un ciberespacio más seguro mediante el intercambio de información de alertas, vulnerabilidades, amenazas y eventos; la mejora de las capacidades de contrainteligencia, la seguridad de sus productos y tecnologías, y la concienciación y formación de sus ciudadanos y servidores públicos en seguridad de sistemas de las Tecnologías de la Información y Comunicaciones (TIC).

Para ello, identifican los actores y responsabilidades presentes en un escenario de ciberseguridad, establecen unos principios comunes de actuación, proponen las líneas de acción para alcanzar como nación las

capacidades necesarias de ciberdefensa y crean las estructuras de decisión y coordinación y los flujos de información necesarios para coordinar la prevención y respuesta ante los ciberataques.

Finalmente, en la mayoría de ellas impulsan el desarrollo de los sistemas de alerta y prevención adecuados que les permitan disponer de una visión de conjunto sobre este problema.

En España, durante los últimos 10 años se han desarrollado iniciativas parciales (criterios de seguridad, conservación y normalización, Centro Criptológico Nacional, infraestructuras críticas, Instituto Nacional de Tecnologías de Comunicación o esquema nacional de seguridad) que se pasarán a describir con las que se intenta mitigar el riesgo de recibir cualquier tipo de ataque procedente de este nuevo tipo de amenaza.

AGENTES DE LA AMENAZA

Los posibles agentes que podrían realizar alguna acción dañina en el ciberespacio son:

– los Estados,
– los grupos extremistas, tanto ideológicos como políticos,
– el crimen organizado y
– las actuaciones delictivas individuales (se tratarán en otro capítulo de este cuaderno).

Estos agentes pueden tener múltiples motivaciones y finalidades: inteligencia, espionaje industrial, propiedad intelectual, motivos políticos, extremismos, motivaciones económicas, etc. Especialmente, los Estados pueden actuar a través de sus servicios de inteligencia, sus unidades cibernéticas de fuerzas armadas, manipulando grupos extremistas afines o contratando mercenarios. Los grupos extremistas ideológicos y políticos se manifiestan normalmente en lo que conocemos por ciberterrorismo.

Destacamos las siguientes manifestaciones, por su impacto en el ciberespacio actual:

– **Crimen Organizado.** Estas organizaciones realizan actividades relacionadas con el robo de información de tarjetas de crédito o de los certificados digitales asociados, con el fraude telemático asociado a operaciones bancarias o a cualquier transacción desde Internet, con el blanqueo de dinero y con el robo de identidades asociado a inmigración ilegal.

- **Espionaje industrial.** Son compañías o gobiernos que tienen interés en disponer de información crítica de desarrollos tecnológicos e industriales de industrias de la competencia.
- **Hacking Político / Patriótico.** Este tipo de actividad recogida abundantemente en prensa es el reflejo de un conflicto regional, étnico, religioso o cultural en el ciberespacio. Así son frecuentes los ataques de denegación de servicio entre China y Japón; Azerbaiyán y Turquía; India y Pakistán, chiitas y sunitas o el conflicto entre árabes e israelíes. Normalmente no tiene un gran impacto en los sistemas de información del País o área que recibe el ataque pues la actividad normalmente se limita a ataques realizados contra servicios Web y no alcanza los sistemas internos.
- **Servicios de Inteligencia.** Se considera el principal vector de amenaza contra la información sensible o clasificada manejada por los sistemas de información gubernamentales y de empresas nacionales de sectores estratégicos (y especialmente aquellas relacionadas con Defensa). Disponen de medios y recursos técnicos y una gran capacidad de acción. Sus actividades son muy prolongadas en el tiempo y el tipo de herramientas que utilizan normalmente muestran unos niveles muy bajos de detección en los sistemas de seguridad de los sistemas objetivos.
- **Unidades cibernéticas de Fuerzas Armadas.** Pueden ser un vector de amenaza crítico sobre todo en tiempo de crisis o conflicto. Muchas naciones disponen de esta capacidad sólo en los servicios de inteligencia aunque en otras, las FFAA,s disponen de unidades que tienen asignadas misiones de ataque a los sistemas de información de los adversarios. Estas unidades son la evolución de las capacidades de inteligencia de señales (SIGINT) disponibles en las FFAA,s de muchos países.
- **Terrorismo.** Los grupos terroristas emplean el ciberespacio como una herramienta más para realizar sus actividades delictivas. Normalmente lo emplean para establecer comunicaciones entre sus células y grupos de apoyo, para obtener información de posibles objetivos, para realizar acciones de propaganda o para obtener financiación a sus actividades.

Algunos de estos agentes suelen contratar capacidades técnicas de ataque disponibles en el mercado negro ofertadas por hackers y organizaciones criminales si no disponen de la capacidad tecnológica necesaria y podrían, en su caso, manipular usuarios internos para disponer de

la información o las credenciales necesarias con las que acceder a los sistemas de información objetivos desde dentro.

En muchas publicaciones se han clasificado estos agentes de la amenaza en 3 grandes grupos, el ciberespionaje, el ciberterrorismo y el cibercrimen. Se trataran brevemente en este capítulo los dos primeros.

Ciberterrorismo

Para que una actividad sea calificada de terrorismo se requiere que sus autores pertenezcan, actúen o colaboren con bandas armadas, organizaciones o grupos cuya finalidad sea la de subvertir el orden constitucional o alterar gravemente la paz pública, mediante la comisión de delitos de estragos, incendios, atenten contra las personas, o recolecten fondos.

Existe mucho debate doctrinal sobre si un terrorista puede realizar acciones violentas que produzcan efectos catastróficos y pánico empleando únicamente ciberataques. No obstante el ciberterrorismo se puede definir como el realizado por medios cibernéticos. Aunque esta definición no solo se extiende al objetivo último de estos grupos sino al empleo de Internet para conseguir los mismos.

Por ello, actualmente las actividades del terrorismo nacional e internacional en el ciberespacio se ciñen principalmente a lo especificado en el apartado anterior y su capacidad de realizar ciberataques a sistemas conectados a Internet es considerada limitada por lo que no parece probable que realice ataques a gran escala sobre los mismos. El impacto de estos ataques sería muy limitado en alcance tanto si el objetivo es la propia red de Internet como si lo son los sistemas conectados a esta red.

Sobre sistemas conectados a Internet y como se tratará posteriormente se destaca que los sistemas de control industrial (SCADA) podrían ser vulnerables a ataques de alcance limitado pero que podrían a llegar a ser críticos puntualmente. El impacto podría ser grave si alcanzan a interrumpir la funcionalidad principal de estos sistemas. En algunos casos el nivel real de interconexión entre el sistema de control industrial (que deberían estar aceptablemente aislado) es muy elevado y podrían ser alcanzados por un atacante (ya se ciberterrorista como otro agente de la amenaza). Además, el impacto en la confianza en los sistemas que produciría un ataque de este tipo, aunque fuera de muy pequeña escala sería muy alto si tiene el eco de los medios de comunicación.

De todas formas, dado el nivel tecnológico que se atribuyen a estos grupos, el ataque con medios tradicionales (explosivos improvisados, ataques suicidas…) se considera mucho más probable que el empleo de herramientas complejas de ciberataques.

Por otro lado, con la rápida evolución de la amenaza, el riesgo de un ciberataque terrorista tiene una tendencia leve a incrementarse y además, podrían actuar otros actores (que se describirán posteriormente) utilizando la cobertura del terrorismo tanto nacional como internacional para ejecutar estas actividades.

Además la actividad terrorista internacional emplea INTERNET como una herramienta más que le ayuda a cumplir sus objetivos. Existen importantes foros como el GIMF (1) que desde hace algunos años realizan actividades de propaganda para el terrorismo internacional. Desde estos y otras páginas Web se lanza el mensaje yihadista. Además, se está utilizando cada vez más asiduamente las redes sociales como Facebook (2) o Twitter (3), u otras redes de distribución de contenidos (Youtube (4)) para mandar sus mensajes de propaganda.

Las capacidades antiterroristas de los gobiernos tratan de limitar las posibilidades de estos grupos de realizar propaganda por Internet intentando clausurar las páginas Web que albergan contenidos que atentan contra la seguridad de las naciones. Ante estas acciones las páginas Web relacionadas directamente con este tipo de actividad migran a alojamientos muchos más robustos a acciones de cierre legal de su actividad. Por las diferencias en el tratamiento de estos delitos en las regulaciones nacionales y por la ausencia de una legislación internacional unificada en esta materia es posible la supervivencia de páginas Web vinculadas directa o indirectamente a organizaciones terroristas.

Otra actividad relevante del terrorismo internacional es la utilización de Internet para realizar acciones de propaganda (publicación de ficheros de audio, video y texto). En esta actividad, además de los mensajes

(1) Global Islamic Media Front (GIMF). Foro de propaganda de radicalismo islámico. www.globaljihad.net/

(2) Facebook. Se creó en 2004, en la actualidad esta red social cuenta con más de 500 millones de usuarios activos. www.facebook.com

(3) Twiter. Se creó en 2006, en la actualidad esta red social cuenta con más de 100 millones de usuarios activos. Se basa en mensajes de texto de 140 caracteres tipo SMS. www.twiter.com

(4) Youtube. Red de descarga de contenidos. www.youtube.com

tradicionales, los ciberterroristas están alerta ante cualquier difamación del Islam y sus símbolos para montar campañas de propaganda incitando a luchar por el orgullo y las creencias maltratadas. Esta actividad se ha reflejado en prensa en los movimientos ante la quema de ejemplares del Corán o la publicación de artículos que difamaban al profeta (5). En esta actividad se pueden encuadrar las numerosas acciones de suplantación de páginas Web y ataques de denegación de servicio en países donde se han realizado afrentas graves a las creencias islámicas.

El objetivo final de esta actividad es conseguir la radicalización del numeroso grupo de jóvenes musulmanes que ya utilizan Internet como medio de relación fundamental.

Se detectan numerosos sitios en Internet que tienen como objetivo apoyar el proceso de radicalización de algunos jóvenes. En estas páginas se encuentra la información necesaria para la formación ideológica y el refuerzo de la misma. Así, en las redes sociales esta actividad se incrementa notablemente. Por tanto, ahora miso es muy difícil diferenciar las actividades de propaganda de las de reclutamiento y radicalización que si se encontrarían fuera de la ley.

En determinadas circunstancias, estas actividades de propaganda o reclutamiento podrían incitar a la realización de actividades de desestabilización promoviendo manifestaciones violentas y actividades ilícitas por lo que su seguimiento por los organismos encargados se hace crucial en los diversos gobiernos.

Otro aspecto a considerar es la obtención de información a través de Internet de posibles objetivos y sus localizaciones especialmente centrada en organizaciones y personas susceptibles de ser atacadas por estos grupos. Con la cantidad de información que las organizaciones y los particulares publican en sus páginas Web, Blogs o redes sociales la obtención de información previa para realizar cualquier tipo de actividad terrorista se facilita enormemente. En el proceso de planeamiento los reconocimientos sobre el terreno se agilizan también por la información que publican aplicaciones como Google Maps (6) y sus nuevos servicios de fotografía satélite y fotografía de itinerario desde el punto de vista de un transeúnte en las diferentes localidades que disponen de este servicio.

---

(5) Caso de quema del Corán. Septiembre 2010. Ha sido recogida en muchos medios. Fecha de consulta 27 de octubre de 2010. www.abc.es/20100909/internacional/islam-clama-contra-quema-20100909.html

(6) www.google.es/map/

Por otro lado la obtención de financiación, aunque posible, es, hasta el momento, muy limitada en alcance aunque se sigue esperando que el ciberterrorismo realice actividades similares a las del crimen organizado (cibercrimen) para obtener una financiación adicional que soporte su actividad fundamental.

Otra actividad para la que se puede utilizar Internet por grupos terroristas es la de formación de sus integrantes y grupos de apoyo, aunque, hasta ahora la red se emplea más en tareas de archivo y almacenamiento de información que en tareas de instrucción on line pues, la necesidad de realizar prácticas e interactuar con los alumnos no está cubierta en esta modalidad de formación.

También destaca el empleo de Internet para establecer comunicaciones de una manera cifrada (mediante el empleo de aplicaciones del tipo PGP (7) o Truecrypt (8)) o enmascarada (empleo de herramientas de esteganografía que ocultan información en otros ficheros soporte) en otras comunicaciones legítimas. Todos los países han establecido regulaciones de interceptación legal de las comunicaciones que cubren tanto los medios tradicionales (telefonía móvil o fija) como el envío de datos a través de Internet. Los terroristas son conscientes de la vulnerabilidad de sus medios de comunicación y realizan acciones para intentar proteger estos.

De todas formas la agilidad y versatilidad que les permite Internet hace que para gran cantidad de sus comunicaciones sea empleado como medio principal, evitándose su uso solo para las que consideran de una criticidad muy elevada por ser acciones que están próximas a ejecutarse.

> *En conclusión, la posibilidad de combinar ataques físicos a infraestructuras de Internet con ataques cibernéticos complejos es poco probable por el nivel tecnológico del ciberterrorismo pero el empleo de Internet para actividades de propaganda, reclutamiento y comunicaciones se ha incrementado por los nuevos servicios que están a disposición como las redes sociales. También es de destacar la obtención de información a través de esta red.*

(7) Pretty Good Privacy (PGP o GnPG en su versión en Linux). Programa popular de cifrado. www.pgp.com

(8) TrueCrypt. Programa de cifrado. www.truecrypt.org

Ciberespionaje

Los ciberataques más sofisticados se esperan de los servicios de inteligencia y las agencias de operaciones de información militares extranjeras. En la mayoría de los casos, estos atacantes disponen de muchos recursos, tienen la paciencia necesaria para encontrar la debilidad del sistema y durante la explotación del ataque intentan lograr la mayor persistencia en el mismo instalando puertas traseras en previsión de una posible detección del mismo.

El objetivo de estos ataques es el mismo que la actividad de inteligencia que lo soporta, adquirir ventaja política, económica, comercial o militar con la información adquirida en los sistemas atacados.

Todos los estados del primer mundo que soportan sus actividades en sistemas de información y que necesitan la interconexión con Internet para alcanzar mayores cotas de eficiencia son susceptibles de recibir este tipo de ataques que intentan alcanzar la información clasificada o sensible, información privada de alto valor o secretos industriales.

Muchos Estados han declarado públicamente que el ciberataque puede ser empleado como una herramienta más de sus estrategias de inteligencia o militares. En este sentido su objetivo final es tanto la exfiltración de información del enemigo como la inutilización o destrucción de los sistemas enemigos tanto para evitar el mando y control de sus fuerzas como para causar daños en sus servicios esenciales y en su población.

La constatación clara de esta realidad es que en los últimos años se han detectado numerosos intentos de agresión, muchos de ellos exitosos, sobre sistemas sensibles de diferentes naciones en el ámbito de la UE y la OTAN. Como ejemplo algunas naciones como Estados Unidos, Reino Unido, Alemania o Francia han declarado públicamente haber recibido ataques muy graves con impactos serios sobre la información sensible manejada en los sistemas de sus respectivos gobiernos. Seguramente muchos otros gobiernos y empresas han recibido ataques similares que no se han hecho públicos.

Por ello se cree imprescindible la protección de estos sistemas contra ciberataques interesados en la información manejada por los mismos. Esta protección debe preservar tanto la confidencialidad de esta información como la disponibilidad e integridad de ésta. Una de las ac-

tividades críticas a realizar por las diferentes administraciones es incrementar las actividades de monitorización, detección y eliminación de estas agresiones que normalmente requiere un incremento notable en los presupuestos asignados a seguridad.

Asimismo se deben regular las salvaguardas a implementar según el nivel de la información manejada por los sistemas para que el perímetro de protección de todos los sistemas de la administración sea homogéneo y la dificultad a la que se enfrente el atacante sea similar independientemente del organismo al que ataque.

Se deben realizar las mismas actividades en los sistemas de empresas que se consideren estratégicas pues el nivel de amenaza es similar.

En conclusión, el ciberespacio ha reducido la dificultad de entrar en el juego del espionaje y el crecimiento de Internet incrementa la superficie de actuación, por ello, la posibilidad de recibir ataques procedente de otros estados intentando adquirir información sensible o clasificada de su gobierno, información de sus empresas estratégicas es quizás el riesgo más elevado al que se enfrentan las naciones.

INFRAESTRUCTURAS CRÍTICAS

Desde hace una década la seguridad de las infraestructuras críticas vienen ocupando la agenda de los responsables políticos en todo el mundo como un aspecto estratégico para garantizar la propia seguridad de nuestros países y nuestros ciudadanos.

Las Infraestructuras críticas, según se definen en el borrador de legislación pendiente de publicación (9) es el conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación.

Este impacto se mide según unos criterios horizontales que determinan la criticidad de una infraestructura. Se han establecido tres:

1. el **número potencial de víctimas** mortales o de lesiones graves que pueda producir;

(9) Borrador de legislación por el que se establecen medidas para la protección de las infraestructuras críticas. www.cnpic.es. Fecha de consulta 15 de junio de 2010 (estuvo disponible durante 1 mes).

2. el **impacto económico** en función de la magnitud de las pérdidas económicas y/o el deterioro de productos o servicios, incluido el posible impacto medioambiental;
3. el **impacto público**, por la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

Las infraestructuras críticas se agrupan en 12 sectores entre los que se incluyen la Administración, el sector aeroespacial, el sector energético, el de la industria, el nuclear, el de la industria química, las instalaciones de investigación, el de agua, el de la salud, el de transporte, el de alimentación, el financiero y tributario y el de las tecnologías de la información y comunicaciones (10).

Centro Nacional de Protección de Infraestructuras Críticas

La Secretaría de Estado de Seguridad (SES), es el órgano responsable de la dirección, coordinación y supervisión de la protección de infraestructuras críticas (PIC) nacionales, de la creación del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC (11)), como órgano director y coordinador de dichas actividades, y de la determinación, clasificación y actualización del Catálogo de Infraestructuras críticas, de acuerdo con lo dispuesto en el acuerdo de Consejo de Ministros de 2 de noviembre de 2007.

El CNPIC desde su creación ha centrado sus esfuerzos en la elaboración de este catálogo y en el desarrollo de una ley (y normativa asociada) que defina de forma más clara su funcionamiento y con el que se pretende impulsar un importante conjunto de medidas, tanto organizativas como de protección, que reforzarán la eficacia de la coordinación y la cooperación entre todas las Administraciones y las diferentes entidades, organismos gestores o propietarios de infraestructuras que prestan servicios públicos esenciales para la sociedad.

Las funciones principales del CNPIC son las de coordinar la información y la normativa; convertirse en el punto de contacto permanente con los gestores, tanto públicos como privados, de las infraestructuras críti-

(10) Anexo borrador de legislación Protección de infraestructuras críticas: sectores estratégicos y ministerios / organismos del sistema competentes en su protección.
(11) Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). http://www.cnpic-es.es/

cas; dirigir y coordinar los análisis de riesgos; establecer los contenidos mínimos de los planes de seguridad de operador (PSO) y de los planes de protección específicos (PPE) de las infraestructuras críticas; establecer un sistema de mando y control y actuar como punto de contacto con centros similares en todo el mundo.

La normativa que se está desarrollando tiene como objetivos principales dirigir y coordinar las actuaciones en materia de protección de Infraestructuras Críticas, previa identificación y designación de las mismas, impulsando, además, la colaboración e implicación de los organismos propietarios de dichas infraestructuras a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo.

Catálogo de Infraestructuras Críticas

Este catálogo está clasificado de SECRETO, registra las infraestructuras consideradas como críticas y que, en su caso, requieren de especiales medidas de protección. Actualmente existen unas 3.700 infraestructuras críticas, de las que el 80% de ellas pertenecen al sector privado. Asociado a cada infraestructura, esta base de datos especifica las medidas de protección, los planes de reacción y la criticidad de la misma.

Es la herramienta fundamental de trabajo pues además de almacenar toda la información sobre la infraestructura establece el punto de enlace con los operadores, fuerzas y cuerpos de seguridad del Estado (FCSE) y cualquier otro representante del sistema de protección de infraestructuras críticas. Permite la actualización continua y facilita el proceso de la evaluación de la criticidad y del nivel de seguridad de las infraestructuras evaluadas por el CNPIC.

Plan de Protección de Infraestructuras Críticas

Cualquier estrategia de seguridad en estas infraestructuras debe tener como uno de sus elementos centrales prevenir posibles ataques, disminuir la vulnerabilidad y, en el caso de que se produjeran situaciones de crisis que afectaran a las infraestructuras esenciales, minimizar los daños y el periodo de recuperación.

Según el borrador de legislación esta estrategia es el Plan Nacional de Protección de Infraestructuras Críticas en el que se establecen los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones Públicas y para articular las medidas preventivas

necesarias, con el fin de asegurar la protección permanente, actualizada y homogénea del sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

Además establece que se articulen unos planes estratégicos sectoriales basados en un análisis general de riesgos que contemple las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten a cada sector.

A partir de estos planes, cada operador debe articular los planes de Seguridad del Operador (PSO) y los planes de protección específicos (PPE) de sus infraestructuras críticas que asociado al análisis de riesgos de la instalación o sistema, establecerán la adopción de medidas permanentes de protección y de medidas temporales y graduadas, en razón a la amenaza específica que se detecte en cada momento (tanto físicas como de carácter lógico).

La elaboración de esta documentación se encuentra actualmente en su fase inicial y será necesaria una mayor publicación de esta normativa de desarrollo para poder definir de una forma clara los requisitos mínimos de seguridad que deben cumplir las mismas.

Ciberataques en las Infraestructuras Críticas

El borrador de legislación se centra especialmente en contemplar, evitar o minimizar los ataques físicos a las infraestructuras críticas; la única referencia disponible en el borrador a ciberataques es la plasmada en la realización del análisis de riesgos y en la redacción de los planes de protección específicos de las infraestructuras críticas donde se contemplan las amenazas lógicas.

Será necesario un desarrollo del mismo donde se contemplen con mayor detalle las amenazas y vulnerabilidades de estas infraestructuras relacionadas con el ciberespacio pues en la actualidad todas las consideraciones de detalle están centradas en ataques físicos (en su mayoría de carácter terrorista) sobre las mismas.

En otros países se contempla con mucha mayor profundidad la posibilidad de estos ataques identificándolos como un asunto crítico a tratar.

Los ciberataques se plantean con especial criticidad en el sector de Tecnologías de Información y Comunicaciones y en los sistemas de in-

formación y comunicaciones que soportan otros sectores estratégicos como los de la Administración y los sistemas SCADA (Supervisory Control And Data Acquisition, Sistemas de Control de Procesos. Ver glosario).

Sistemas SCADA

En muchos de los sectores estratégicos nombrados, para supervisar y mantener el control de las infraestructuras se utilizan sistemas de control, llamados comúnmente SCADA.

Así, con los sistemas SCADA se controlan los procesos de fábricas químicas, redes eléctricas, centrales de generación eléctrica, industrias de petróleo y gas, tratamiento de agua y residuos e industrias farmacéuticas entre otros.

Hasta hace poco, el relativo desconocimiento de este tipo de sistemas reducía al mínimo sus riesgos de seguridad. No obstante, ya en 2005 se anunció la primera vulnerabilidad de un sistema de control, generando un gran debate acerca de la divulgación de dicha información. Desde entonces, el interés en los sistemas de control industrial ha crecido exponencialmente, en parte como consecuencia de la conexión de éstos con redes de comunicaciones públicas (Internet) y por la incorporación de tecnologías comerciales (equipos de comunicaciones o sistemas operativos entre otros) para maximizar la rentabilidad de las inversiones.

En 2008 aparecieron los primeros programas diseñados para explotar las vulnerabilidades de los sistemas de control industrial. En 2009 y 2010 se han detectado ataques a estos sistemas.

El riesgo principal de estos sistemas es el desconocimiento por parte del propietario de las interconexiones reales de los sistemas SCADA, la ausencia de buenas prácticas de seguridad como la realización de actualizaciones periódicas o una adecuada gestión de las contraseñas y las deficiencias en la configuración de los diferentes dispositivos que proporcionan muchas posibilidades de realizar acciones remotas que permiten el control de los mismos.

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN OTROS PAÍSES

En este apartado se van a analizar algunas estrategias de seguridad publicadas oficialmente siempre desde el punto de vista defensivo. Es-

tos documentos, en sus versiones públicas, no tratan el aspecto ofensivo del ciberespacio y no se analizarán en este apartado.

Se presentan las aproximaciones de las naciones que han presentado públicamente las soluciones para abordar este problema.

Estados Unidos

Las dimensiones y estructuras creadas en Estados Unidos no son comparables a las del resto de los países.

Tras los ataques del 11 de septiembre de 2001 se impulsaron las estrategias de una defensa territorial más activa y coordinada que finaliza en la creación de un Departamento de Seguridad del Territorio Nacional (12) (noviembre de 2002). Asimismo se desarrolla una amplia legislación relacionada con la ciberseguridad y la protección de infraestructuras críticas.

La estrategia de Seguridad Nacional en el Ciberespacio (13) de febrero 2003 asigna la responsabilidad de la protección al DHS y reconoce que debe ser un esfuerzo coordinado de los gobiernos federal, estatal y local, del sector privado y de los ciudadanos. Establece 5 líneas estratégicas prioritarias a las que asigna responsables y acciones de detalle a realizar para alcanzarlas:

1. **Sistema de respuesta nacional de seguridad en el ciberespacio**. Para ello propone diversas acciones, entre las que destacan, la mejora de la gestión de incidentes, ampliar el sistema de alerta ante ciberataques, realizar ejercicios de coordinación o mejorar el intercambio de información público-privado.
2. **Programa de reducción de amenazas y vulnerabilidades**. Para ello propone diversas acciones, entre las que destacan, la mejora de las capacidades de las fuerzas de seguridad (FBI (14) y otras agencias policiales, la mejora del control de los sistemas SCADA o profundizar en el conocimiento sobre amenazas y vulnerabilidades.
3. **Formación y concienciación en el ciberespacio**. Este programa estaba preparado para cinco tipos de audiencias; ciudadanos y pequeñas empresas, empresas consideradas estratégicas (especialmente las que gestionan infraestructuras críticas), universida-

(12) Department of Homeland Security (DHS) www.dhs.gov
(13) The National Strategy to Secure Cyberspace. White House. www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
(14) Federal Bureau of Investigation. (FBI). www.fbi.gov

des y centros de investigación (especialmente los que dispongan de gran capacidad de cálculo), sector privado (especialmente el que disponga de sistemas SCADA) y gobiernos locales y estatales.

4. **Asegurar el ciberespacio gubernamental**. Las acciones a realizar en el gobierno federal fueron el seguimiento de la evolución de las amenazas y vulnerabilidades y la implementación de las mejoras de seguridad adaptadas a estas, el impulso de la alianza nacional para asegurar la información (NIAP) (15), la mejora de la seguridad de las redes sin cables, la mejora de los requisitos de seguridad en la subcontratación y en las adquisiciones y la mejora en la realización de los procesos de auditoría o inspección. Además se debe impulsar la seguridad en los gobiernos locales y estatales.
5. **Cooperación nacional e internacional.** Como líneas de actuación destacan el refuerzo de las actividades de contrainteligencia, la mejora de las capacidades de prevención y atribución de un ataque y la coordinación entre las diferentes agencias. Internacionalmente se intentará mejorar los canales de comunicación y que se adopten en las legislaciones nacionales los acuerdos sobre cibercrimen.

La estrategia de Seguridad Nacional en el Ciberespacio de 2003 asigna responsabilidades que descansan en su mayoría en el DHS y dispone de un completo anexo con las acciones recomendadas para cada línea estratégica.

Para el desarrollo de esta estrategia, dentro del DHS, se impulsa el US-CERT (16) que proporciona apoyo en la respuesta ante ciberataques contra la parte civil del gobierno federal (.gov) y tendrá la responsabilidad de relacionarse con los gobiernos locales, estatales y la industria.

Destaca que el DHS tiene además, la misión de protección de infraestructuras críticas nacionales definida en el acta de 2002 (17).

En el ámbito del Ministerio de Defensa (DoD) (18) existen muchas iniciativas tanto de los tres ejércitos como de las agencias de inteligencia que tienen misiones en la protección de las redes sensibles y clasificadas

(15) National Information Assurance Partnership (NIAP). Iniciativa para evaluar las tecnologías de información entre el Nacional Institute of Standards and Technology (NIST) y la National Security Agency (NSA).

(16) US-CERT. http://www.us-cert.gov/

(17) Critical Infrastructure Information Act of 2002. http://www.dhs.gov/xlibrary/assets/CCI_Act.pdf

(18) Department of Defense (DoD) www.dod.gov

como la Agencia de Seguridad Nacional (NSA) (19). Esta agencia tiene un departamento encargado del aseguramiento de la información (NSA-IAD (20)) que se focaliza en el análisis permanente de nuevas amenazas y vulnerabilidades, en el desarrollo de guías, productos y soluciones de seguridad, en el desarrollo de productos de cifra y gestión de claves de los mismos y en la formación y concienciación de seguridad.

El DoD financia el CERT-CC (21) que tiene como una de sus misiones principales establecer un foro de coordinación entre CERT,s nacionales. Esta operado por la Universidad Carnegie Mellon) y su misión principal es la relación con otros CERT,s (especialmente gubernamentales) para intercambiar información y colaborar ante incidentes de seguridad.

Con el presidente Obama se han reforzado las iniciativas en ciberseguridad. Con su llegada y tras un periodo de revisión de 60 días, la Casa Blanca (22) en mayo de 2009 publicó la revisión de la política en el ciberespacio (23) en la que demanda una visión de conjunto y reconoce que debido a la disparidad de misiones de las diferentes agencias, el gobierno federal no se encuentra preparado para este desafío. Por ello la estrategia nacional se debe orientar a mejorar la resistencia ante ciberataques y a reducir la ciberamenaza. En el documento se establecen 10 acciones urgentes a ejecutar inmediatamente.

1. Nombramiento de un responsable de ciberseguridad nacional que coordine todas las políticas y actividades de las diferentes agencias. Se crea una oficina dependiente del consejo de seguridad Nacional (NSC) que le apoyará en estas tareas.
2. Actualizar y aprobar una nueva estrategia que asegure las infraestructuras de comunicaciones nacionales.
3. Designar la ciberseguridad como una de las prioridades del Presidente.
4. Designar un responsable de privacidad y libertades públicas en el NSC.
5. Desarrollar los mecanismos de coordinación entre las diferentes agencias y establecer claramente las responsabilidades de éstas.

(19) National Security Agency (NSA) www.nsa.gov
(20) National Security Agency. Information Assurance Directorate (IAD).
(21) CERT-CC. Centro de coordinación de CERT. Establecido en la Universidad Carnegie Mellon en 1988. www.cert.org
(22) White House. www.whitehouse.gov/administration/eop/nsc/cybersecurity
(23) Cyberspace Policy Review. www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

6. Realizar campañas nacionales de concienciación y formación.
7. Mayor implicación del gobierno de los Estados Unidos en la regulación internacional de la ciberseguridad que permita una mayor colaboración internacional.
8. Preparar un plan de respuesta ante incidentes de seguridad.
9. Potenciar las capacidades de investigación y desarrollo en este campo.
10. Asegurar la privacidad y las libertades civiles.

El objetivo último de estas acciones a corto plazo es conseguir una visión de conjunto y coordinar las acciones de los diferentes actores. Además, propone otras 14 acciones para el medio plazo entre las que destacan las de mejora de los recursos humanos y técnicos disponibles en el gobierno federal, la coordinación entre agencias y los controles en el presupuesto para alcanzar los objetivos marcados.

Para conseguir la plena consecución de los objetivos marcados, se refuerza la Iniciativa global sobre ciberseguridad nacional (CNCI) (24) elaborada por el Presidente Bush en enero de 2008 (clasificada en su momento) que establece los siguientes 3 objetivos estratégicos para conseguir un ciberespacio más seguro:

– **Establecer una línea de defensa contra todas las amenazas actuales.** Para ello se debe mejorar el intercambio de información de alertas, vulnerabilidades amenazas y eventos que se detecten en el gobierno federal, en el resto de gobiernos estatales y locales y en el sector privado que permitan actuar rápidamente para reducir estas y prevenir las intrusiones.
– **Defenderse contra todo el espectro de amenazas.** Por ello se deben mejorar las capacidades de contrainteligencia e incrementar la seguridad en las cadenas logísticas y en los productos y tecnologías desde su fase de diseño.
– **Fortalecer el entorno futuro de ciberseguridad.** Para ello se deben extender la formación y concienciación en seguridad, coordinar y dirigir los esfuerzos de investigación y desarrollar estrategias que disuadan la actividad hostil en el ciberespacio.

(24) Comprehensive National Cybersecurity Initiative (CNCI) lanzada por el Presidente George W. Bush en la «National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)» en enero de 2008. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Esta aproximación está dotada de los fondos necesarios para que las fuerzas de seguridad y las comunidades de inteligencia y defensa mejoren funciones críticas como la recolección, proceso y análisis de información. El responsable de ciberseguridad nacional debe supervisar que se ejecuten las siguientes iniciativas:

1. **Gestión de las redes del gobierno federal como una red única** con conexiones seguras a Internet. Asigna esta responsabilidad al DHS y al GAO (25).
2. **Finalizar el despliegue de un sistema de sensores de detección de intrusos en toda la red del gobierno federal (EINSTEIN 2)**. Son sensores pasivos que utilizan tecnologías de detección basadas en firmas. Es operado por el US-CERT (DHS). Este sistema permite detectar cualquier actividad dañina y mejora el conocimiento de las vulnerabilidades de la red corporativa. Se ha realizado un estudio sobre el impacto en la privacidad de los datos del sistema (26).
3. **Iniciar el despliegue de un sistema Prevención de intrusos (EINSTEIN 3).** Es una mejora del sistema anterior con la capacidad de actuación en tiempo real sobre el tráfico dañino. Se colaborará con la NSA (según lo previsto en la ley) para realizar la monitorización de contenidos si es necesario y además ésta proporcionará nuevos patrones de ataque desarrollados dentro de sus misiones de recolección de información y de aseguramiento de la información. Ya existe un piloto basado en tecnología aportada por esta agencia.
4. **Coordinar y redirigir los esfuerzos de investigación y desarrollo**. Se desean eliminar redundancias y se crearán estructuras que coordinen y prioricen las inversiones tanto para sistemas clasificados como no clasificados.
5. **Interconexión de centros de operaciones de seguridad** para mejorar el intercambio de información y la visión de conjunto de las amenazas que se produzcan. Se asigna esta misión al Centro de Operaciones de Ciberseguridad (NCSC) (27) del DHS que integrará la información de los 6 centros que proporcionan actualmente este servicio.

---

(25) Government Accountability Office (GAO). www.gao.gov

(26) Privacy Impact Assessment for EINSTEIN 2. US-CERT. 19 de mayo 2008. www.dhs.gov/

(27) National Cybersecurity Center (NCSC).

6. **Desarrollar en todo el gobierno federal un plan de contrainteligencia cibernética.** Con esta acción se pretende detectar, disuadir y mitigar cualquier ataque realizado por los servicios de inteligencia extranjeros contra la información, los sistemas gubernamentales y los del sector privado.
7. **Aumento de seguridad de las redes clasificadas.** Estas redes manejan la información más sensible de la Administración para dirigir las operaciones de paz, las actividades diplomáticas, las actividades contraterroristas, las actividades de las FCSE o de inteligencia así como las actividades de seguridad interior.
8. **Extender la cibereducación**. Se detecta una falta de personal con las capacidades técnicas adecuadas en este campo. Los programas actuales se consideran limitados y faltos de visión global. Se considera que se deben impulsar estos perfiles al igual que en los años 50 se impulsaron los perfiles de ciencias y matemáticas.
9. **Definir y desarrollar nuevos programas, estrategias y tecnologías que refuercen la seguridad**.
10. **Definir y desarrollar nuevos programas y estrategias que refuercen la disuasión** desarrollando respuestas adecuadas ante amenazas estatales y no estatales.
11. **Desarrollar una aproximación global a la gestión de riesgos en la cadena logística de las tecnologías de información y comunicaciones**. Se requiere mayor concienciación de este problema y el desarrollo de una nueva política de adquisiciones que se adapte al nuevo mercado global de estas tecnologías intentando que se adapten a los estándares y buenas prácticas de referencia.
12. **Definir el papel del gobierno para mejorar la ciberseguridad en los sectores que manejan infraestructuras críticas**. Esta misión la tiene asignada el DHS pero se fuerza a realizar un programa con unos hitos tangibles a corto y medio plazo.

De la estrategia de ciberseguridad de 2003, la CNCI de 2008 y de la revisión de la política del ciberespacio de 2009 destaca el sentido práctico, al elevar el nivel tratamiento del problema desde el DHS a la Casa Blanca con el responsable designado al efecto y la decisión de coordinación de todos los esfuerzos nacionales.

En las 7 primeras propuestas de la CNCI se apuesta por alcanzar objetivos tangibles. Las dotaciones presupuestarias asignadas a la

misma reflejan la importancia de esta estrategia para el gobierno americano.

Además, en la revisión de 2009 se asigna una función más activa y operativa a las agencias de inteligencia, en especial a la NSA, por su conocimiento profundo de la ciberamenaza y las nuevas tendencias de ataque.

Reino Unido

La Estrategia de Ciberseguridad en el Reino Unido (28) fue publicada en junio de 2009 y tiene como objetivo asegurar las ventajas de este país en el ciberespacio mediante tres líneas estratégicas:

– Reducción del riesgo del uso del Ciberespacio por el Reino Unido actuando sobre la amenaza (disminuyendo su motivación y capacidad), sobre sus vulnerabilidades y sobre el impacto de cualquier ataque en los intereses nacionales.
– Aprovechar las oportunidades en el ciberespacio mediante la obtención de inteligencia que apoye las políticas nacionales y actué contra los adversarios.
– Incrementar las actividades de concienciación, desarrollar una doctrina sobre el ciberespacio y sus políticas derivadas y mejorar las capacidades humanas y técnicas.

El documento considera que al igual que en el siglo XIX para alcanzar la seguridad nacional se tuvieron que asegurar los mares y en el XX el aire, en el XXI se debe asegurar la ventaja en el ciberespacio y ése es el objetivo al que apunta esta estrategia.

Asimismo, implícitamente se considera que actualmente las misiones en este campo se encuentran dispersas en diversos organismos que no están coordinados entre sí. Así se pueden destacar los siguientes:

– La Oficina del Consejo de Ministros (29). En ella se encuentra la Secretaría de Seguridad Nacional así como otros organismos relacionados con ciberamenazas entre los que destaca el jefe de la información gubernamental.

(28) Cyber Security Strategy of the United Kingdom. June 2009. Cabinet Office. www.cabinetoffice.gov.uk
(29) Cabinet Office. www.cabinetoffice.gov.uk

– El Centro Nacional de Protección de Infraestructuras Críticas (CPNI)(30) que proporciona asesoramiento en seguridad a empresas y organizaciones que gestionan infraestructuras críticas. Este centro depende del Servicio de Seguridad Interior (MI5) (31) que actúa contra cualquier amenaza organizada contra la seguridad nacional.
– La agencia de inteligencia en las comunicaciones y de aseguramiento de la información (GCHQ (32) / CEGS(33)) con la misión de obtención de inteligencia de señales y de protección de las redes gubernamentales.
– El Ministerio del Interior (Home Office (34)) con la misión de luchar contra el uso del ciberespacio por parte de cualquier actividad criminal. Dispone de la oficina de seguridad y contraterrorismo que lucha específicamente contra el uso terrorista del ciberespacio.
– El Ministerio de Defensa (35) con misiones relacionadas con el uso militar del Ciberespacio.
– El Servicio de inteligencia (36) con la misión de proporcionar inteligencia exterior de fuentes humanas para defender la seguridad nacional y el bienestar económico del Reino Unido.
– La Policía Metropolitana (37) con sus unidades de cibercrimen.
– La Agencia del crimen organizado (SOCA) (38) para el uso del ciberespacio por parte del crimen organizado.

Por ello, se propone que se establezca un programa que afecte a todo el gobierno para alcanzar los objetivos estratégicos incrementando los fondos que desarrollen nuevas tecnologías para proteger las redes nacionales, incrementando la formación para conseguir personal con perfiles adaptados a esta actividad y trabajando coordinadamente con el sector público, la industria, los grupos de defensa de las libertades civiles, los ciudadanos y los aliados internacionales.

(30) Centre for the Protection of National Infrastructure (CPNI) www.cpni.gov.uk
(31) British Security Service(BSS-MI5) www.mi5.gov.uk
(32) Government Communications Head Quarter (GCHQ) www.gchq.gov.uk
(33) CEGS Communications-Electronics Security Group www.cegs.bov.uk. Creado en 1969.
(34) Home Office / Office for Security and Counter-Terrorism (OSCT) www.homeoffice.gov.uk
(35) Ministry of Defence www.mod.uk
(36) Secret Intelligence Service (SIS-MI6). www.sis.gov.uk
(37) Metropolitan Police www.met.police.uk
(38) Serious Organised Crime Agency (SOCA) www.soca.gov.uk

Asimismo, con la misión de coordinar todos los esfuerzos, se crean los siguientes organismos:

– Oficina de Ciberseguridad (OCS) (39) dentro de la Oficina del Consejo de Ministros encargada del desarrollo de esta estrategia que debe impulsar las acciones parciales de otros organismos. Su objetivo es proporcionar liderazgo y coherencia en la aplicación de la misma. Asimismo se fijan 8 líneas de acción. Esta oficina se ha unificado con la de Aseguramiento de la Información también existente en este organismo pasándose a denominarse OCSIA (40). El personal destinado es aportado por los diferentes organismos con responsabilidades en el ciberespacio.
– El Centro de operaciones en ciberseguridad (CSOC) (41) liderado por el GCHQ y ubicado en su sede institucional. Está constituido por las diferentes agencias con responsabilidades en este terreno con la misión de proporcionar el estado de alerta, analizar tendencias y mejorar la coordinación en la respuesta técnica ante ciberincidentes. De la actividad de este organismo se informará a un panel interdepartamental que se organizará en el CEGS que es la autoridad y el brazo ejecutor de las políticas de aseguramiento de la información (Information Assurance).

La dotación presupuestaria recibida asciende a 650 millones de libras en 4 años (42) en un momento en que se están anunciando los mayores recortes de inversiones desde la segunda guerra mundial.

> *De esta estrategia se destaca la importancia que se otorgan a las implicaciones de seguridad del ciberespacio, la voluntad del gobierno británico de coordinar los esfuerzos de sus diferentes agencias, y la determinación de invertir presupuesto para adquirir capacidades en un campo que considera estratégico para adquirir ventaja en futuros conflictos.*
>
> *La estructura y división de funciones en ciberseguridad existentes actualmente en el Reino Unido es en muchos casos similar a la existente en España.*

(39) Office of Cyber Security (OCS) www.cabinetoffice.gov.uk
(40) Office of Cyber Security and Information Assurance (OCSIA). www.cabinetoffice.gov.uk
(41) Cyber Security Operation Centre (CSOC).
(42) Anuncio del Nuevo presupuesto y de la estrategia Nacional de Ciberseguridad. http://direct.gov.uk/produc_consum_dg/groups/dg_digitalassets/

Canadá

La Estrategia de Ciberseguridad en Canadá (43) fue publicada en 2010 y resalta la importancia del ciberespacio para el modo de vida de los canadienses. Destaca la facilidad y efectividad de los ataques y señala como principales riesgos el ciberespionaje y las actividades militares de otros estados, el uso terrorista de Internet y el cibercrimen. Además resalta la continua evolución de las amenazas lo que requiere una defensa que se adapte a esta circunstancia.

La estrategia se basa en tres pilares:

– Securización de los sistemas gubernamentales. Para ello se deben articular las estructuras, herramientas y personal necesarios para cumplir este objetivo.
– Cooperación con los gobiernos provinciales y regionales y con el sector privado para apoyar iniciativas que mejoren la resistencia de los sistemas nacionales haciendo especial énfasis en las infraestructuras críticas.
– Ayudar a los canadienses a proteger sus actividades en el ciberespacio reforzando las capacidades contra el cibercrimen de las fuerzas de seguridad del Estado.

La estrategia resalta además, la necesidad de trabajar conjuntamente con la comunidad académica, las organizaciones no gubernamentales y el sector privado para intentar mejorar la seguridad de los sistemas canadiense.

Posteriormente la estrategia desarrolla los tres pilares. Se designa al Ministerio de seguridad pública de Canadá (44) y a su Centro de Respuesta ante Ciberincidentes (45) que debe continuar con la misión de monitorizar y apoyar a los diferentes organismos ante cualquier incidente de seguridad informático.

En apoyo de este organismo la Agencia de Seguridad de las Comunicaciones (46), el servicio de inteligencia (47), la policía montada (48), el

(43) Canada´s Cyber Security Strategy. www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.aspx
(44) Public safety Canada. www.publicsafety.gc.ca
(45) Canadian Cyber Incident Response Centre. www.publicsafety.gc.ca/prg/ccirc
(46) Communications Security Establishment. www.cse-cst.gc.ca
(47) Canadian Security Intelligence Service. www.csis-scrs.gc.ca
(48) Royal Canadian Mounted Police. www.rcmp-grc.gc.ca

secretariado del tesoro (49), el Ministerio de Asuntos Exteriores y tratados internacionales (50) y finalmente, el Departamento de Defensa Nacional y las Fuerzas Armadas Canadienses (51) le proporcionaran toda la información disponible sobre la amenaza.

Además se establece la necesidad de mejorar la arquitectura de seguridad de los sistemas gubernamentales y la reducción de las interconexiones con Internet. Se recuerda la necesidad de que los diferentes departamentos monitoricen y aseguren sus operaciones electrónicas como se establece en la política de seguridad publicada en 2009.

En el desarrollo del segundo y tercer pilar se dan ejemplos de la necesidad de cooperación y se alerta sobre los riesgos de los sistemas SCADA y se propone la realización de ejercicios para depurar la coordinación entre los diferentes gobiernos y compañías. Además se realizarán acciones que mejoren la cultura de seguridad de los canadienses y se creará el centro de fusión del cibercrimen con el que se espera mejorar la capacidad de la policía montada en este campo.

Esta estrategia destaca que la ciberseguridad es una responsabilidad compartida y para el desarrollo de los tres pilares es fundamental el trabajo coordinado. La implantación de esta estrategia tiene una asignación presupuestaria inicial de 90 millones de dólares en cinco años y 18 millones adicionales.

> *Canadá al igual que Estados Unidos, Reino Unido y Australia ha considerado crítica esta actividad publicando una estrategia que aborda el problema de forma global y concentrando las misiones en el Ministerio de seguridad pública. No define claramente los mecanismos de coordinación con el resto de organismos.*

Francia

La estrategia francesa sobre ciberseguridad la establece el libro blanco de la seguridad y Defensa Nacional (52) aprobado por el Presidente de la República en junio de 2008 donde se resalta que la ciberamenaza

(49) Treasury Board Secretariat. www.tbs-sct.gc.ca
(50) Foreign Affaire and International Trade Canada. www.international.gc.ca
(51) Department of National Defence. www.forces.gc.ca
(52) Livre blanc sur la défense et la sécurité nationale. www.livreblancdefenseetsecurite.gouv.fr/information

tiene una probabilidad muy alta de que se produzca y su impacto en las infraestructuras críticas y en los sistemas gubernamentales es considerado alto.

Este libro blanco contempla cinco funciones estratégicas que las fuerzas de defensa y seguridad francesas deben dominar que son: el conocimiento y la previsión (con la necesidad de mejora de las capacidades técnicas de las Agencias de Inteligencia), la prevención (con la necesidad de una defensa proactiva en profundidad que realice una vigilancia permanente), la disuasión, la protección y la respuesta.

Anteriormente a esta estrategia se había desarrollado un plan de mejora de la Seguridad de los Sistemas de Información del Estado (53) desde el 2004 al 2007.

En Francia la Secretaria General de la Seguridad y Defensa Nacional (54) dependiente del primer Ministro y recientemente reestructurada, es la encargada de tratar todos los asuntos de ciberdefensa y dentro de ésta en julio de 2009 se creó la Autoridad Nacional de Seguridad de los Sistemas de Información (ANSSI) (55) con las siguientes misiones:

- La detección y reacción urgente ante ciberataques mediante la vigilancia continua de las redes gubernamentales sensibles y la implementación de mecanismos de defensa en estas redes.
- El desarrollo de productos y servicios de confianza para su uso en los gobiernos y en los sectores críticos.
- Proporcionar asesoramiento de seguridad a organismos gubernamentales y operadores de infraestructuras críticas.
- Proporcionar información a empresa y ciudadanos sobre las nuevas amenazas a la seguridad de la información y el procedimiento de protección mediante una política activa de comunicación.

Entre los organismos subordinados destacan la subdirección de estrategia y reglamentación, el centro de formación y el centro operacional

(53) Consultar en Cuadernos Cátedra ISDEFE-UPM. Nº 6 Seguridad Nacional y Ciberdefensa. Octubre 2009. Anexo A. Punto 1.4.2.

(54) Secrétariat général de la défense et de la sécurité nationale SGDSN www.sgdsn.gouv.fr/

(55) Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 (Journal officiel du 8 juillet 2009). www.ssi.gouv.fr

de la seguridad de los sistemas de información (COSSI) (56), en disponibilidad permanente, que aglutina misiones de desarrollo de productos de cifra, realización de inspecciones y auditorías de seguridad a sistemas gubernamentales, realización de ejercicios que evalúen la seguridad, despliegue de sistemas de detección y, en caso de crisis, coordinación de la respuesta gubernamental.

En el COSSI se encuentra además el centro de expertos del gobierno en el tratamiento de ataques informáticos (CERTA) (57) creado en 1999 y que hacía las funciones de CERT gubernamental y los observatorios regionales de seguridad de los sistemas de información (OzSSI) (58) que facilitan la aplicación de buenas prácticas y mejoran la atención a los usuarios en todo el territorio.

> *Con la nueva orgánica de la SGDSN y la creación de la ANSII en 2009 en Francia se han centralizado todas las actividades críticas relacionadas con la ciberdefensa en busca de una respuesta más eficaz y operativa ante ciberataques. Asimismo la ANSII ha recibido una importante dotación presupuestaria.*

Alemania

No está disponible ninguna estrategia de ciberseguridad alemana. No obstante en 1990 se creó la Oficina federal de Seguridad de la Información (BSI) (59) dependiente del Ministerio Federal de Interior (BMI) (60). Anteriormente estas funciones las realizaba el servicio de inteligencia (BND) (61).

Las misiones del BSI son la de protección de las redes del gobierno federal (incluye el CERT-Bund, el centro de situación de las tecnologías de información, el centro de gestión de crisis y los sistemas de alerta temprana), el desarrollo de productos de cifra, el análisis de nuevas tecnologías, la seguridad de los productos software (SW) y la protección de infraestructuras críticas.

---

(56) Centre opérationnel de la sécurité des systèmes d'information (COSSI). www.ssi.gouv.fr

(57) CERTA Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques www.certa.ssi.gouv.fr/

(58) OzSSI Observatoires zonaux de la sécurité des systèmes d´information

(59) BSI www.bsi.bund.de

(60) BMI www.bmi.bund.de

(61) BND. www.bnd.bund.de

El BSI opera el CERT-Bund (62) como CERT gubernamental desde 2001 e impulsa una alianza de todos los equipos de respuesta ante incidentes alemanes denominada CERT-Verbund (63). Además el BSI soporta el CERT para ciudadanos y pequeñas y medianas empresas denominado Bürger-CERT (64).

También tienen misiones en la protección de infraestructuras críticas la Oficina Federal de protección civil y asistencia ante desastres (BBK (65)) y la agencia federal de policía criminal (BKA (66)).

En el BMI se ha organizado un grupo de trabajo interministerial de infraestructuras críticas (AG KRITIS (67)) que establece los escenarios de riesgo, realiza análisis de vulnerabilidades en sectores críticos, propone contramedidas y supervisa los sistemas de alerta temprana.

El Plan nacional de protección de infraestructuras de la información (68) se marca como objetivos la prevención (las actividades críticas son divulgar información sobre riesgos y posibilidades de protección o empleo de productos y sistemas confiables), la preparación (las actividades críticas son recolectar y analizar información y proporcionar alertas y avisos) y de reacción (mejorar las capacidades técnicas propias y desarrollar productos con tecnología nacional).

> *Aunque no dispone de estrategia de ciberseguridad publicada todas las misiones defensivas ante ciberataques se concentran en el BSI que dispone de varios equipos de respuesta ante incidentes para proporcionar este servicio. No se espera que se publique más normativa. Durante los últimos años se han incrementado sus recursos humanos y económicos para proporcionar nuevos servicios tanto a Administraciones Públicas y ciudadanos como a empresas que gestionan infraestructuras críticas.*

---

(62) CERT-Bund. www.bsi.bund.de/certbund/

(63) CERT.Verbund. www.cert-verbund.de/

(64) Bürger-CERT (2007). www.buerger-cert.de

(65) BBK. www.bbk.bund.de

(66) BKA. www.bka.bund.de

(67) No hay informes publicados sobre AG KRITIS. Se encuentra una versión en borrador (alemán) //userpage.fu-berlin.de/~bendrath/Kritis-12-1999.html.

(68) Federal Ministry of the Interior. «National Plan for Information Infrastructure Protection» (Berlin, 2005). www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure_ Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.

Estonia

Este país dispone de una estrategia de seguridad publicada en mayo de 2008 (69). En la que se plantea como objetivo reducir las vulnerabilidades de su ciberespacio a través de la implementación de los planes nacionales específicos (entre 2008-2013) y de la colaboración internacional. Planea sobre el documento el ataque generalizado recibido en abril-mayo en 2007. El comité que desarrolló la estrategia, liderado por el Ministerio de Defensa contaba también con expertos del sector privado.

La misión de desarrollar esta estrategia es del Ministerio de Defensa en cooperación con el Ministerio de Educación e Investigación, el Ministerio de Justicia, el Ministerio de Economía, el Ministerio del Interior y el Ministerio de Asuntos Exteriores. No obstante el consejo de ciberseguridad supervisa estas actividades.

Los objetivos estratégicos a conseguir son:

– Aplicar de forma gradual un conjunto de medidas de seguridad. Este objetivo afecta a infraestructuras críticas (se fijan 10 sectores), Internet y sistemas SCADA. Se deben mejorar las capacidades de detección y respuesta ante incidentes así como la coordinación entre agencias nacionales.
– Desarrollar conocimiento técnico mediante el desarrollo de normativa que mejore la formación en seguridad, la realización de ejercicios y el impulso a iniciativas de investigación y desarrollo en ciberseguridad.
– Desarrollar el marco normativo y legal que soporte el empleo seguro de los sistemas de información y la protección de infraestructuras críticas.
– Promover la colaboración internacional para fortalecer la ciberseguridad de tal forma que se condenen los ciberataques por el daño que ocasionan a derechos humanos y a las libertades democráticas. Para ello se intentarán impulsar acuerdos internacionales contra ciberataques y cibercrimen.
– Concienciación en seguridad de la información a todos los niveles pero con especial atención a ciudadanos y pequeña y mediana empresa.

(69) Cyber Security Strategy for 2008–2013. Cyber Security Strategy Committee. Ministry of Defence. ESTONIA. Tallinn 2008. http://www.mod.gov.ee/en/national-defense-and-society

Para asegurar el cumplimiento de los objetivos se establecen plazos muy concretos para el desarrollo de los planes específicos y se ha creado un consejo de ciberseguridad dependiente del Comité de Seguridad del Gobierno de la República que informa del estado de cumplimiento mediante informes anuales.

> *Se han concentrado en el Ministerio de Defensa la responsabilidad de desarrollar esta estrategia aunque hay otros cinco ministerios involucrados y un consejo de ciberseguridad al más alto nivel que vigila su aplicación... Destaca el detalle de las medidas específicas a desarrollar para cumplir con los objetivos estratégicos y el plazo de cinco años para conseguirlos.*

Australia

Este país dispone de una estrategia de seguridad publicada el 23 de noviembre 2009 (70) como resultado de la revisión estratégica del gobierno electrónico realizada en 2008 y presentada por el Primer Ministro en el Parlamento en diciembre de 2008.

Esta estrategia se basa en unos principios básicos, unos objetivos y unas prioridades estratégicas.

Los principios básicos son:

– **Liderazgo nacional** para afrontar la escala y complejidad del desafío de la ciberseguridad.
– **Responsabilidad compartida** de todos los ciudadanos para mantener sus equipos seguros.
– **Colaboración** del sector público, el sector privado y de todos los ciudadanos.
– **Compromiso de colaboración internacional.** Debido a la naturaleza transnacional de Internet se requiere una acción global para conseguir un acuerdo en ciberseguridad.
– **Gestión de riesgos**. Al tener un ciberespacio interconectado, la vulnerabilidad de los sistemas ante ciberataques hace que una protección completa sea imposible. Por ello se debe realizar una aproximación basada en la gestión de riesgos para priorizar las actividades a realizar.
– **Protección de los valores y libertades fundamentales**. Se debe perseguir que las políticas en ciberseguridad sean respetuosas con estos valores individuales y colectivos.

(70) Cyber Security Strategy. www.ag.gov.au/cybersecurity.

Los objetivos del gobierno australiano con esta política de ciberseguridad son:

1. Que todos los australianos sean conscientes de los riesgos, aseguren sus equipos y protejan su privacidad, identidad y gestiones financieras en sus actividades on-line.
2. Que las compañías australianas operen de forma segura y que sus sistemas de información y comunicaciones protejan la integridad de sus operaciones y la identidad y privacidad de sus clientes.
3. Que el gobierno australiano asegure su información y que sus sistemas de información y comunicaciones sean seguros y resistentes.

Para conseguir estos objetivos, las prioridades estratégicas son:

– Mejorar la capacidad de detección, análisis y respuesta ante ciberataques sofisticados centrándose en sistemas gubernamentales, de infraestructuras críticas y otros de interés nacional.
– Concienciar y ayudar a los australianos proporcionando información y herramientas prácticas para su protección on-line (71).
– Colaborar con el sector privado para promover la seguridad y resistencia de sus infraestructuras, redes, productos y servicios (72).
– Implantar las mejores prácticas en los sistemas gubernamentales priorizando aquellos que proporcionen servicios on-line. Entre las medidas de desarrollo destaca el estudio para la reducción de los accesos a Internet y la colaboración activa con los gobiernos locales y regionales para que los requisitos de interconexión sean comunes.
– Promover un entorno electrónico seguro, resistente y de confianza que proteja los intereses nacionales.
– Mantener un marco legal y unas capacidades en las fuerzas de seguridad que permitan la persecución efectiva del cibercrimen.
– Promover el desarrollo de una comunidad de investigación en ciberseguridad que permita el desarrollo de soluciones innovadoras en este campo mediante la estrategia nacional de seguridad en ciencia e innovación.

Para abordar estas prioridades, la estrategia establece que se deben potenciar dos organizaciones, ya existentes, que deben alcanzar una capacidad operativa completa en 2010.

---

(71) www.staysmartonline.gov.au
(72) Foro de intercambio de información sobre infraestructuras críticas. www.tisn.gov.au

El primero de ellos es el CERT nacional (CERT Australia (73)) que pasa a depender de la Fiscalía General (74) y que unificará todas las capacidades en este campo en torno al anterior CERT gubernamental (GovCERT.au (75)). Será el que proporcione toda la información necesaria en ciberseguridad (en especial sobre amenazas y vulnerabilidades) a la comunidad nacional y actuará como punto de contacto para las relaciones internacionales. Deberá establecer canales seguros para el intercambio de información entre el sector público y privado y tendrá la misión de coordinar nacionalmente cualquier incidente de seguridad crítico.

El segundo de ellos es el Centro de Operaciones en Ciberseguridad (CSOC (76)) perteneciente a la agencia de inteligencia de señales (DSD (77)). Este centro reúne personal de diferentes agencias de seguridad. Dispone de un amplio conjunto de fuentes en todos los dominios; inteligencia, seguridad, fuerzas policiales, equipos de respuesta ante incidentes (nacionales y del sector privado) que le permiten disponer de una visión completa de los sistemas de información australianos. Coordina la respuesta ante incidentes complejos entre las diversas agencias del gobierno y proporciona el nivel de alerta nacional.

Además la estrategia involucra a los siguientes organismos que deben proporcionar toda la información necesaria a las dos organizaciones arriba apuntadas:

– El Departamento del Fiscal General que proporciona las políticas en ciberseguridad y contra el cibercrimen.
– La Autoridad Australiana de comunicación y medios (78) responsable de la regulación de las telecomunicaciones y canal de enlace con los proveedores de servicios para actuar contra amenazas como el spam, el robo de identidades o la infecciones de ordenadores.

(73) CERT Australia. www.cert.gov.au

(74) Attorney-General's Department. www.ag.gov.au/. Agencia que lidera la política de ciberseguridad para todo el gobierno australiano. Preside el comité de coordinación y políticas en ciberseguridad (Cyber Security Policy and Coordination (CSPC) Committee) que es el comité interdepartamental encargado de coordinar el desarrollo de las políticas de ciberseguridad.

(75) Australian Government Computer Emergency Readiness Team (GovCERT.au). www.cert.gov.au.

(76) Cyber Security Operations Centre (CSOC).

(77) Defence Signals Directorate (DSD). www.dsd.gov.au/

(78) Australian Communications and Media Authority (ACMA). www.acma.gov.au

– La Policía federal australiana (79) que está encargada de todos los crímenes tecnológicos complejos y que coordina en este campo a todas las fuerzas policiales australianas y se relaciona con los organismos internacionales en este campo.
– Las Agencias de inteligencia y seguridad (80) que según las funciones establecidas en su ley (81) de 1979 debe, entre otras misiones, investigar los ataques electrónicos con propósitos de espionaje, sabotaje o terrorismo; recolectar inteligencia sobre ciberataques contra sistemas del gobierno e infraestructuras críticas o proporcionar la correspondiente evaluación de la amenaza en este campo.
– La agencia de inteligencia de señales (DSD) que según las funciones establecidas en su ley (82) es la autoridad nacional de seguridad para los sistemas de información gubernamentales proporcionando consejo y orientación en las mejores prácticas de seguridad (mantiene el manual de seguridad de los sistemas de Información y Comunicaciones gubernamentales y proporciona productos de cifra certificados) y, a través del CSOC, es responsable de los servicios ya enumerados en éste.
– El departamento de economía digital y comunicaciones (83) responsable de potenciar el empleo de la economía digital alineando las iniciativas privadas de ciberseguridad con las gubernamentales.
– La Oficina de gestión de información del Gobierno en el departamento de economía (84).

En mayo de 2008 se ha realizado una asignación presupuestaria de 125,8 millones de dólares en cuatro años para incrementar la seguridad en el plan de seguridad cibernética (www.dbcde.gov.au) para la protección contra delitos de cibercrimen. En el presupuesto de 2009 se ha realizado una asignación presupuestaria de 100 millones de dólares (dentro de los 685 dedicados a seguridad nacional) (85) para impulsar los obje-

(79) Australian Federal Police **(**AFP). www.afp.gov.au
(80) Australian Security Intelligence Organisation**'s** (ASIO). www.asio.gov.au
(81) *Australian Security Intelligence Organisation Act 1979*
(82) *Intelligence Services Act 2001.* www.dsd.gov.au/
(83) Department of Broadband, Communications and the Digital Economy (DBCDE). www.dbcde.gov.au/
(84) Department of Finance and Deregulation's Australian Government Information Management Office (AGIMO). www.finance.gov.au/agimo/
(85) Información sobre el presupuesto (fecha consulta 11.10.2010) www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Budgets_Budget2009_MediaReleases_StrengtheningOurNationalSecurity.htm

tivos y prioridades marcados en la estrategia como la concentración de todas las capacidades de CERT (dotado con 8,8 millones).

> *Esta estrategia nacional considera la ciberseguridad una de las prioridades nacionales, marca unos objetivos y prioridades a conseguir y reforma las responsabilidades nacionales concentrando en la Fiscalía general (CERT Australia) y en la agencia de inteligencia de señales (CSOC) los esfuerzos de protección activa contra ciberataques.*
>
> *La estrategia está acompañada de una importante dotación presupuestaria y el resto de departamento tiene la obligación de colaborar y apoyar con todos los medios necesarios en su consecución.*

Organizaciones Internacionales

La organización y actividades de OTAN y UE se han tratado en otros capítulos de este cuaderno.

En la UE resalta el dictamen del Comité Económico y Social Europeo sobre «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia» (86) que propone un plan de acción basado en 5 pilares; preparación y prevención, detección y respuesta (mecanismos de alerta temprana), mitigación y recuperación, cooperación internacional e identificación de infraestructuras críticas.

En este documento la UE exhorta a las naciones a la creación de equipos de respuesta ante incidentes nacionales y su adhesión al grupo de CERT gubernamentales europeos (EGC (87)).

Conclusiones

Del análisis de estas estrategias se extraen las siguientes conclusiones:

– Se realiza una aproximación global al problema tratando de forma conjunta todos los niveles sobre los que se debe actuar en ciberdefensa:
  • Gobiernos centrales, regionales y locales.
  • Infraestructuras críticas
  • Fuerzas y cuerpos de seguridad del Estado
  • Ciudadanos

(86) [COM(2009) 149 FINAL] (2010/C 255/18) Dictamen. C/255 de 22.09.2010.
(87) European Government CERT http://www.egc-group.org/

– Se reconoce que es un problema emergente, que el escenario es incierto, que es una de las prioridades para la seguridad nacional y como tal, se debe abordar.
– En las naciones analizadas, se centralizan las responsabilidades en ciberdefensa en uno o dos organismos o en un una oficina de coordinación cuya dependencia es del presidente o primer ministro o, en su caso, se fortalece de forma explícita la posición de los organismos a los que se asigna esta misión.
– Se potencian las capacidades de monitorización y alerta temprana, se concentran y se fortalecen los equipos de respuesta ante incidentes (especialmente las gubernamentales) por considerarlos los mejor posicionados para resolver el problema de las nuevas amenazas de forma más eficiente.
– Se impulsan esquemas nacionales de seguridad (requisitos de seguridad mínimos a implantar en las redes gubernamentales) y se intentan disminuir las interconexiones con Internet.
– Se priorizan y fortalecen las capacidades de inteligencia por el mejor conocimiento que poseen de la amenaza con el objetivo de hacer frente a ataques complejos.
– Se declara como necesidad estratégica la formación y concienciación de servidores públicos, empresas y ciudadanos. Se presentan diversas soluciones para conseguir este objetivo.
– Se impulsan las actividades de investigación e innovación en este campo mediante alianzas con Universidades y centros de investigación.
– Se proporciona una dotación presupuestaria para la implantación de las estrategias con la vocación política de mantenerla en el tiempo.

ESPAÑA. RESPONSABILIDADES EN EL CIBERESPACIO

Tras el análisis de las soluciones propuestas por los diferentes países y como distribuyen las responsabilidades en el ciberespacio. Se analizan éstas en los siguientes organismos:

– Ministerio de Industria, Turismo y Comercio (88).
– Ministerio del Interior(89).
  • Secretaría de Estado de Seguridad. CNPIC (90).

(88) Ministerio de Industria Turismo y Comercio. www.mityc.es
(89) Ministerio del Interior. www.mir.es/
(90) Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). www.cnpic-es.es/

  - Unidades de investigación tecnológica de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).
- Ministerio de Política Territorial y Administración Pública (91).
  - Consejo Superior de Administración Electrónica (CSAE (92)).
- Centro Nacional de Inteligencia (93)
  - Autoridad Nacional de Seguridad Delegada (94)
  - Centro Criptológico Nacional (95)
- Ministerio de Defensa (96).
  - Dirección General de Infraestructuras
  - Estado Mayor de la Defensa
  - Cuartes Generales de Tierra, Armada y Aire.

Ministerio de Industria Turismo y Comercio

Este Ministerio a través de su Secretaría de Estado de Telecomunicaciones y Sociedad de la Información tiene entre otras misiones, la de relacionarse con los operadores de telecomunicaciones, la gestión de nombres del dominio.***es***, la capacidad de dictar normas sobre interceptación legal de comunicaciones y el desarrollo de la sociedad de la información con el plan Avanza (impulsa el empleo de las tecnologías de información en la sociedad). En el RD (97) que define su estructura básica se referencia alguna misión genérica en seguridad de la información.

Dispone de organismos con responsabilidades en desarrollo de sociedad de la información como Red.es (98) y en seguridad, accesibilidad y calidad como INTECO (99) que a su vez disponen de sendos equipos de respuesta ante incidentes que se describirán posteriormente.

---

(91) Ministerio de la Política Territorial y Administración Pública. www.mpt.es
(92) Consejo Superior de Administración electrónica (CSAE). www.csae.map.es/
(93) Centro Nacional de Inteligencia (CNI). www.cni.es
(94) Autoridad Nacional de Seguridad Delegada (ANS-D). Ver funciones en página Web CNI. www.cni.es
(95) Centro Criptológico Nacional (CCN). www.ccn.cni.es
(96) Ministerio de Defensa. www.mde.es/
(97) RD 1620/2010 el que se regula su estructura básica del MITYC. www.mityc.es
(98) RED.ES. Empresa pública empresarial adscrita al M. Industria, Turismo y Comercio a través de la Secretaria de Estado de Telecomunicaciones y Sociedad de la Información que tiene por misión impulsar la sociedad en red en España. www.red.es
(99) Instituto Nacional de Tecnologías de la Comunicación (INTECO). www.inteco.es

Ministerio del Interior

La Secretaria de Estado de Seguridad es el organismo en este ministerio con competencias en el ciberespacio a través del CNPIC y de las unidades encargadas de la ciberdelincuencia en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

El CNPIC tiene responsabilidades en la protección de estas infraestructuras con las salvedades especificadas en el borrador de legislación que se encuentra en elaboración (Protección Civil, MINISDEF, FCSE, Aviación Civil, Consejo de Seguridad Nuclear y funciones del CNI que se complementarán con este centro). Tiene la responsabilidad de custodiar, mantener y actualizar el Plan Nacional de Protección de Infraestructuras Críticas y el Catálogo Nacional de Infraestructuras Estratégicas.

El CCN-CERT (100) colabora con el CNPIC en el tratamiento de los ciberataques sobre infraestructuras críticas y en la actualización de información sobre vulnerabilidades SCADA e incidentes de seguridad informáticos relacionados con infraestructuras críticas. Se debe esperar a la aprobación de su legislación y la elaboración de normativa de detalle para definir responsabilidades ante ciberincidentes en estas infraestructuras.

Respecto a las FCSE con responsabilidad en la ciberdelincuencia existen 2 unidades que desarrollan esta tarea, el Grupo de delitos telemáticos (101) de la Guardia Civil y la Brigada de Investigación Tecnológica (BIT) (102) de Cuerpo Nacional de Policía. En las policías autonómicas (País Vasco, Navarra y Cataluña) existen unidades que tratan este tipo de delitos.

Ministerio de Política Territorial y Administración Pública

Este ministerio (103) preside el Consejo Superior de Administración Electrónica (104) y a través de éste, debe promover la colaboración y cooperación con las comunidades autónomas y las entidades locales para

(100) Capacidad de respuesta ante incidentes gubernamental. www.ccn-cert.cni.es
(101) Grupo de Delitos telemáticos (DGT). www.gdt.guardiacivil.es/
(102) Brigada de Información Tecnológica (BIT). www.policia.es/bit/
(103) Estas funciones han sido desarrolladas por el anterior Ministerio de Administraciones Públicas y posteriormente en el Ministerio de Presidencia. En la última remodelación del gobierno de octubre de 2010 estas competencias se han traspasado al Ministerio de Política territorial y Administración Pública.
(104) Consejo Superior de Administración Electrónica (CSAE). www.csae.map.es/

la puesta en marcha de servicios públicos interadministrativos. Para ello preside la conferencia sectorial de las AAPP que reúne a todas las CCAA y la conferencia nacional de la Administración local (para ayuntamientos de más de 140.000 habitantes).

Además debe impulsar las actividades de cooperación de la Administración General del Estado con la Unión Europea, con las organizaciones internacionales y, especialmente, con Iberoamérica, en materia de tecnologías de la información y Administración electrónica, en colaboración con el Ministerio de Asuntos Exteriores y de Cooperación. Por otro lado, gestiona la red SARA (105).

Consejo Superior de Administración Electrónica

El Consejo Superior de Administración Electrónica (106) es el órgano encargado de la política y estrategia del Gobierno en materia de tecnologías de la información y la implantación de la Administración Electrónica en la Administración General del Estado. Dispone de una comisión permanente cuyas funciones se detallan en el Real Decreto 589/2005, de 20 de mayo.

En colaboración con el Centro Criptológico Nacional el CSAE realizará las siguientes acciones:

– Elaboración de medidas de seguridad de las tecnologías de la información y comunicaciones,
– Adquisición coordinada de material de cifra
– Formación de personal especialista en seguridad de los sistemas

Dispone de un Observatorio de la Administración Electrónica (107) que analiza el nivel de implantación de ésta en las AAPP.

---

(105) Sistemas de Aplicaciones y Redes para las Administraciones (SARA). Artículo 43. Ley 11/2007 de 22 junio. Acceso de los ciudadanos a los servicios públicos. Establece la interconexión de las diferentes Administraciones para intercambio de información y servicios y para la interconexión con la Unión Europea y otros Estados miembros. www.ctt.map.es/web/proyectos/redsara

(106) El Consejo Superior de Administración Electrónica, «es el órgano colegiado adscrito al Ministerio de Administraciones Públicas –hoy Ministerio de la Presidencia- encargado de la preparación, la elaboración, el desarrollo y la aplicación de la política y estrategia del Gobierno en materia de tecnologías de la información» (Art. 3 del Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados de la Administración Electrónica).

(107) Observatorio de la Administración electrónica. www.obsae.map.es/

Centro Nacional de Inteligencia

El CNI depende orgánicamente del Ministerio de Defensa pero en la seguridad de la información clasificada y en el ámbito de la ciberdefensa tiene encuadrados a organismos que tienen misiones que afectan a todas las Administraciones Públicas.

El Secretario de Estado Director del CNI es Autoridad Nacional de Seguridad Delegada (ANS-D) por el Ministro de Defensa y Ministro de Asuntos Exteriores para la protección de información clasificada Nacional e Internacional. Tiene como órgano de trabajo para esta actividad a la Oficina Nacional de Seguridad (ONS) (108) y por la ley 11/2002, de 6 de mayo, reguladora del CNI es Director del Centro Criptológico Nacional.

Oficina Nacional de Seguridad

La ONS se crea en 1983. Tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España.

Destacan las siguientes funciones:

- Realización de Acuerdos para protección de la Información Clasificada a nivel internacional.
- Participación en Comités y Grupos de Trabajo sobre protección de información clasificada de Unión Europea, OTAN, acuerdos internacionales y programas clasificados.
- Relaciones con otras Autoridades Nacionales de Seguridad.
- Expedición de Habilitaciones Personales de Seguridad.
- Expedición de Habilitaciones de Empresa.
- Acreditación y autorización de los Órganos, Instalaciones y Sistemas que manejan Información Clasificada.

En la acreditación de sistemas para manejar información clasificada trabaja conjuntamente con el CCN en apoyo de la ANS-D.

Centro Criptológico Nacional

Fue creado en el año 2004, a través del Real Decreto 421/2004. Comparte con el CNI medios, procedimientos, normativa y recursos. A su vez,

(108) Oficina Nacional de Seguridad (ONS). www.cni.es/es/ons/

y tal y como contempla el Real Decreto citado anteriormente, al CCN están adscritos el Organismo de Certificación (OC (109)) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) y la capacidad de Respuesta a Incidentes de Seguridad de la Información en las Administraciones Públicas (CCN-CERT).

Las funciones establecidas en el RD 421/2004 son:

- Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC en la Administración
- Formar al personal de la Administración especialista en el campo de la seguridad de las TIC
- Constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito
- Valorar y acreditar la capacidad de productos de cifra y Sistemas de las TIC (que incluyan medios de cifra) para manejar información de forma segura
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los Sistemas antes mencionados
- Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia (Sistemas de las TIC)
- Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países.

El RD 3/2010 por el que se regula el Esquema Nacional de Seguridad reitera estas funciones, esta vez, para los sistemas sujetos a la Ley 11/2007 de Administración Electrónica. Destacando el desarrollo de normativa en apoyo al esquema (Artículo 29) y las misiones encomendadas al CERT Gubernamental (Artículos 36 y 37).

Ministerio de Defensa

Además de las misiones que tiene asignada el CNI este Ministerio dispone de un elevado número de sistemas clasificados y gestiona diversos sistemas de intercambio de información y mando y control con OTAN. Dispone de una política de seguridad con responsabilidades sobre sistemas que manejan información clasificada.

(109) Organismo de Certificación. www.oc.ccn.cni.es

Las responsabilidades se encuentran distribuidas en Dirección General de Infraestructuras (DIGENIN(110)), en el Estado Mayor de la Defensa (EMAD) y en los Cuarteles Generales de los tres Ejércitos.

Dirección General de Infraestructuras

Destaca la misión de dirigir y coordinar la planificación, obtención y gestión de los sistemas de información y telecomunicaciones, así como la política de seguridad de la información. Entre sus unidades destacan la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones y la Subdirección General de Servicios Técnicos y Telecomunicaciones que gestiona entre otras la red corporativa del Ministerio.

Estado Mayor de la Defensa

El Estado Mayor de la Defensa es responsable del planeamiento, dirección y control del Sistema de Mando y Control Militar de las FAS, y de las telecomunicaciones que lo soportan. Es Autoridad Delegada de Acreditación para los sistemas conjuntos que manejen información nacional clasificada.

Cuarteles Generales

Son responsables de los sistemas propios. Son Autoridades Delegadas de Acreditación para los sistemas propios que manejen información nacional clasificada.

Equipos de Respuesta ante Incidentes

Actualmente, los equipos de respuesta ante incidentes se consideran los organismos con mayor capacidad técnica y con la estructura más adecuada para luchar contra el mayor espectro de ciberamenazas. El modo de actuación es muy colaborativo y sus relaciones son informales y flexibles pero guiadas por criterios de máxima eficiencia y rapidez en la actuación.

La descripción que se refleja a continuación no es exhaustiva y solo intenta proporciona una visión general de los campos de actuación de los equipos que se encuentran operando. Se relacionan a continuación:

(110) Dirección General de Infraestructuras (DIGENIN). www.mde.es/organizacion/organigramaMinisterio/secretariaEstado/

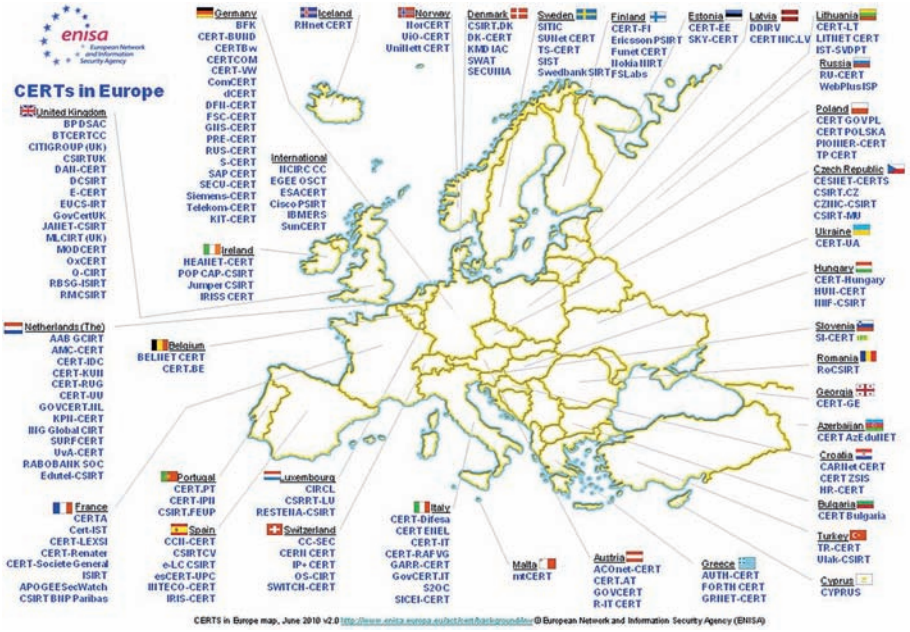
– **CCN-CERT** (111)**.** (Organismo adscrito al CCN-CNI). Tiene responsabilidades en ciberataques sobre sistemas clasificados, sistemas de la Administración General, Autonómica y Local y, en coordinación con el CNPIC, sobre sistemas que gestionen infraestructuras críticas. Proporciona el estado de la amenaza en ciberseguridad para Presidencia de Gobierno. Este CERT es el CERT gubernamental/nacional. Tiene esta responsabilidad reflejada en el RD 3/2010 de 8 de enero que desarrolla el Esquema Nacional de Seguridad. En los artículos 36 y 37 se asigna a este CERT el papel de coordinador público estatal.
– **INTECO-CERT** (112) (Instituto Nacional de Tecnologías de Comunicación adscrito al Ministerio de Industria, Turismo y Comercio). Tiene responsabilidades de seguridad y respuesta ante incidentes de seguridad en los entornos de ciudadanos y pequeñas y medianas empresas (PYMES) según la definición de la comunidad sobre la que actúa este CERT. En su creación 2004 se le traspasó el CATA (Centro de Alerta Temprana Antivirus) desde Red.es, empresa pública también adscrita al Ministerio de Industria.
– **CERT en comunidades autónomas (CCAA).** Existe creado y reconocido el CSIRT-CV (113) de la Generalitat Valenciana y están en fase de despliegue / desarrollo, el CESICAT (114) (CERT de la Generalitat Catalana) y el ANDALUCIA-CERT. Estos organismos dependen de sus CCAA respectivas. Las responsabilidades de estos CERT,s es diferente pudiéndose referir a los sistemas de la administración autonómica y/o local así como tener otras misiones de asistencias a empresas y ciudadanos. Se debe consultar su misión y objetivos en las páginas Web correspondientes.
– **IRIS-CERT** (115)**.** Organismo adscrito al Ministerio de Industria, Turismo y Comercio. Tiene responsabilidades de seguridad en la red IRIS que da servicio a la comunidad universitaria y a los centros de investigación.
– **Otros CERT.** Existen otros CERT y centros operativos de seguridad que ofrecen servicios a otros sectores. Entre ellos destacan por su actividad los siguientes:

(111) CCN-CERT. www.ccn-cert.cni.es
(112) INTECO-CERT. http://cert.inteco.es
(113) Computer Security Incident Response Team (equipo de respuesta ante incidentes de seguridad informática) de la Comunidad Valenciana CSIRT-CV. www.csirtcv.es/
(114) Centro de Seguridad de la Información de Cataluña (CESICAT). www.cesicat.cat/
(115) IRIS-CERT. www.rediris.es/cert/

– **e-La Caixa-CSIRT** (116). Respuesta ante incidentes de seguridad de este banco.
– **S21Sec-CERT** (117). Este CERT proporciona servicios de gestión de incidentes para las diferentes entidades, fundamentalmente, del sector bancario).
– **esCERT-UPC** (118). Decano de los CERT,s nacionales. Fundado en 1994. Proporciona servicios de CERT a la Universidad Politécnica de Cataluña.
– **Hispasec** (119). Empresa de seguridad que proporciona servicios de CERT.

Todos los CERT se coordinan a través del grupo de trabajo de CERT,s nacionales (CSIRT.es) (120) y a su vez, en el foro ABUSES(121) se relacionan con los principales proveedores de servicios de Internet.

En la figura adjunta se muestran los CERT,s recogidos por ENISA (122).



(116) E-La Caixa-CSIRT. www.lacaixa.es
(117) S21Sec-CERT. www.cert.s21sec.com
(118) EsCERT-UPC. http://escert.upc.edu/
(119) Hispasec. www.hispasec.com
(120) CSIRT.es. www.csirt.es
(121) Foro abuses. www.abuses.es/
(122) European Network and Information Security Agency (ENISA). www.enisa.europa.eu/

Relaciones internacionales

En el ámbito internacional existen foros de colaboración entre los organismos responsables de ciberseguridad preferentemente entre los equipos de gestión de incidentes de seguridad de los diferentes países entre los que destacan los siguientes:

- **FIRST** (123). Esta organización relaciona los CERT,s reconocidos de los diferentes países resaltando su misión y la comunidad a la que proporciona servicio. La adscripción a este foro requiere un procedimiento que culmina con una auditoría realizada por uno de los CERT,s que patrocinan la adhesión del nuevo equipo. Los CERT,s nacionales reconocidos por orden de ingreso son Iris-CERT (1997), e-La Caixa-CERT (2005), CCN-CERT (2007), EsCERT-UPC (2007), e INTECO-CERT (2008).
- **TF-CSIRT** (124)**. Grupo de trabajo de TERENA (Trans-European Research and Education Network Association).** Es el foro de CERT,s europeos. Los CERT,s nacionales reconocidos por orden de ingreso son EsCERT-UPC, Iris-CERT, CCN-CERT, INTECO-CERT y CSIRT-CV. Por otro lado, S21Sec-CERT y CESICAT están en proceso de acreditación.
- **European Government CERT** (125)**.** Es el grupo de trabajo de CERT,s gubernamentales/nacionales europeos. La adhesión a este grupo requiere una auditoria formal sobre el mandato legal, la capacidad técnica y los procedimientos empleados por el CERT. En principio solo se admite un único equipo por país. El representante nacional es el CCN-CERT.
- **NCIRC** (126)**. Capacidad de respuesta ante incidentes de OTAN.** Es la capacidad equivalente a los equipos citados anteriormente para OTAN. Identifica al CCN-CERT como CERT nacional para la coordinación de incidentes de seguridad principalmente asociado con ataques o fugas de información sensible. El CCN-CERT participa en los ejercicios de ciberdefensa organizados por este organismo conjuntamente con el Estado Mayor de la Defensa (EMAD).
- **Sistema de Alerta Temprana de la Unión Europea.** Está en proceso de definición desde principios de 2010. Identifica a los CERT,s

(123) Forum for Incident Response and Security Teams (FIRST). www.first.org/
(124) TERENA. www.trusted-introducer.nl/
(125) European Government CERT www.egc-group.org/
(126) NATO Computer Incident Response Capability (NCIRC). www.ncirc.nato.int/

gubernamentales para realizar el intercambio de información y para solicitar colaboración en caso de la detección de un ataque que afecte a más de una nación.

– **Directorio MERIDIAN** (127)**.** Directorio internacional de organismos y agencias gubernamentales con responsabilidad en la protección de infraestructuras críticas. No es específico de los equipos de respuesta ante incidentes aunque en los diversos aspectos que cubre el directorio aparecen estos equipos. En este directorio tienen responsabilidades las siguientes organizaciones; Secretaría de Estado de Seguridad (CNPIC) del Ministerio del Interior, CNI/CCN, Secretaría de Estado de Telecomunicaciones y Sociedad de la Información (SETSI) del Ministerio de Industria Turismo y Comercio, Dirección de Infraestructura y Seguimiento de Situaciones de Crisis (DISCC) de Presidencia del Gobierno y Ministerio de Defensa.

ESPAÑA. SITUACIÓN ACTUAL

Con el panorama citado en el apartado anterior se puede ver que las responsabilidades de seguridad en el ciberespacio están distribuidas en varios organismos tanto en la Administración General de Estado como en la autonómica.

La posibilidad de solapes y sistemas que puedan depender de diversos organismos es muy alta. Además, la respuesta eficaz a las nuevas amenazas que se tienen que afrontar hace necesaria un intercambio de información muy ágil y una coordinación muy estrecha entre los diferentes organismos con responsabilidades.

En los siguientes apartados se amplía información de la problemática asociada a los siguientes ámbitos:

– Actuación de CERT,s
– Sistemas clasificados
– Sistemas de la Administración. Esquema Nacional de Seguridad
– Protección de datos personales
– Sistemas asociados a infraestructuras críticas

(127) International Critical Information Infrastructure Protection Directory. Meridian conference Issue 24. Agosto 2010. No disponible en enlace público. www.meridianprocess.org/

Ámbitos de actuación en ciberseguridad

Por ámbitos la actuación de estos equipos de respuesta ante incidentes sería:

- **Sistemas relacionados con Seguridad y Defensa**. En este ámbito por lo establecido en el RD 421/2004 la responsabilidad recae en el CCN y la respuesta ante incidentes de seguridad en el CCN-CERT. Los sistemas aquí contemplados pertenecen fundamentalmente al Ministerio de Defensa, Ministerio del Interior, Presidencia de Gobierno, Ministerio de Política Territorial y Administración Pública y Ministerio de Asuntos Exteriores y Cooperación. Preferentemente se trata de sistemas que manejan información clasificada. Disponen de regulación propia y se tratarán en apartado correspondiente.
- **Sistemas de las Administraciones Públicas**. Las responsabilidades no se encuentran completamente definidas aunque el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad determina que las responsabilidades de actuación ante cualquier incidente contra estos sistemas se ubican en el CCN-CERT, especialmente para los sistemas recogidos en el ámbito de la ley 11/2007 de Administración electrónica. Iris-CERT da servicio a la comunidad académica.
- **Ciudadano y PYME**. Las actuaciones en estos ámbitos en materia de prevención y respuesta están lideradas por el Ministerio de Industria, Turismo y Comercio (MITYC). La capacidad de respuesta ante incidentes se articula a través del INTECO-CERT aunque los CERT,s de las Comunidades Autónomas también se atribuyen competencias en su demarcación territorial sobre esta comunidad.
- **Operadores de Telecomunicaciones y Proveedores de Servicios**. Los principales operadores y proveedores disponen de centros de operación de seguridad (SOC) orientados hacia la prevención y respuesta ante incidentes de seguridad, fraudes y ataques a sus infraestructuras.
- **Sectores estratégicos / Infraestructuras críticas**. La responsabilidad sobre estos sistemas recae en el CNPIC con las salvedades expuestas en el proyecto de legislación. Existen algunos CERT de carácter privado que dan servicio a alguno de los sectores estratégicos.

Muchos de estos ámbitos de actuación se superponen y, en la gestión de incidentes de seguridad, se detectan solapes y redundancias.

Sistemas Clasificados

Los sistemas que manejan información clasificada tanto nacional como de la OTAN, Unión Europea (UE) o sujeta a acuerdos internacionales disponen de una normativa muy completa y de la obligatoriedad de someterse a un proceso de acreditación en el que se verifican mediante las auditorias correspondientes todos los aspectos relacionados con la seguridad del sistema.

Existe un completo conjunto normativo de requisitos de seguridad según el nivel de clasificación de la información cuando es manejada en estos sistemas, recogido en las series CCN-STIC publicadas por el CCN según lo establece el RD 421/2004 donde se desarrollan las funciones de este organismo.

Tanto en la OTAN como en la UE la interconexión de los sistemas nacionales con los propios requiere una declaración de conformidad firmada de la Autoridad Nacional de Seguridad que debe ejecutar las inspecciones o las auditorias necesarias para la verificación del cumplimiento de todos los requisitos de seguridad establecidos.

A diferencia de lo establecido para la información clasificada de OTAN y UE, España adolece de una normativa de alto nivel que cubre todos los niveles de clasificación. Así en España la ley 9/1968, de secretos oficiales se establecen los niveles de SECRETO y RESERVADO, las clasificaciones de CONFIDENCIAL y DIFUSIÓN LIMITADA solo se han adoptado fruto de los acuerdos internaciones en el reconocimiento de información recibida de organizaciones internacionales. Por ello, solo el Ministerio de Defensa dispone de legislación de detalle que fije los estándares de protección de estos niveles de clasificación.

En el cuadro adjunto (128) se muestran las equivalencias entre las diferentes clasificaciones de seguridad (OTAN, UE, Nacional, Ley Orgánica de Protección de Datos y Esquema Nacional de Seguridad) aunque no se pueden equiparar si puede servir de orientación aproximada del nivel de protección.

(128) CCN-STIC 001 Seguridad de las Tecnologías de Información y comunicaciones que manejan información nacional clasificada en la Administración. Diciembre 2006. www.ccn-cert.cni.es

<table>
<tr><th>NACIONAL</th><th>OTAN</th><th>UE</th><th>LOPD(1)</th><th>ENS</th><th>OTROS(5)</th></tr>
<tr><td>SECRETO</td><td>COSMIC TOP SECRET</td><td>TRES SECRET UE</td><td></td><td></td><td></td></tr>
<tr><td>RESERVADO</td><td>NATO SECRET</td><td>SECRET UE</td><td></td><td></td><td></td></tr>
<tr><td>CONFIDENCIAL</td><td>NATO CONFIDENTIAL</td><td>CONFIDENTIEL UE</td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">DIFUSION LIMITADA</td><td rowspan="2">NATO RESTRICTED</td><td rowspan="2">RESTREINT UE</td><td rowspan="2">ALTO(2)</td><td>ALTO(4)</td><td rowspan="3">USO INTERNO</td></tr>
<tr><td rowspan="2">MEDIO</td></tr>
<tr><td>SIN CLASIFICAR</td><td>NATO UNCLASSIFIED</td><td>-----</td><td>MEDIO(3)
BASICO(3)</td><td>BAJO</td></tr>
</table>

1) Reglamento de aplicación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal
2) Puede incluir algunas protecciones consideradas para información CONFIDENCIAL
3) Entre Básico y Medio existe un nivel intermedio de aplicación
4) No incluye protecciones criptográficas
5) Uso Interno Administración equivalente a DL

Estos sistemas manejan la información más sensible por lo que las medidas de seguridad que deben incorporar deben ser máximas y la vigilancia de los mismos extrema.

Esquema Nacional de Seguridad

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos establece la obligatoriedad de proporcionar los diferentes servicios de la Administración en el Ciberespacio. La ley contempla la creación de sedes electrónicas desde las que los diferentes organismos deben proporcionar el máximo de servicios en línea al ciudadano.

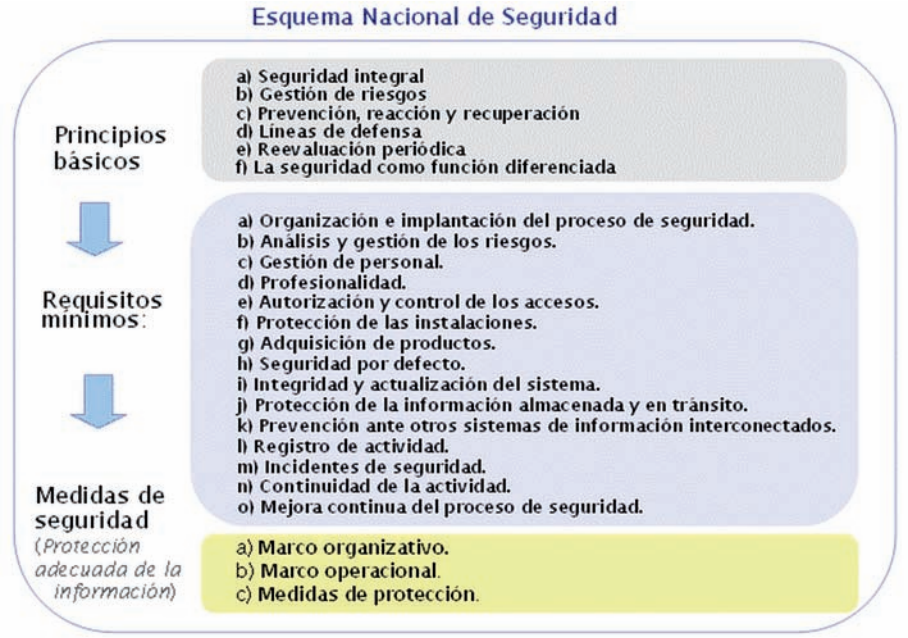
Asimismo establece que las Administraciones Públicas utilizarán las tecnologías de la información asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Esta ley, en su artículo 42, regula la creación de un Esquema Nacional de Seguridad que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por unos princi-

pios básicos y requisitos mínimos que permitan una protección adecuada de la información. Este esquema ha sido publicado en el RD 3/2010 y por primera vez establece un conjunto de medidas de seguridad de obligado cumplimiento según el nivel de la información o sistema (ALTO, MEDIO o BAJO).

Asimismo, como aspectos interesantes del RD resaltan; la obligatoriedad de la realización de auditorías, la recomendación del empleo de productos certificados y la articulación de una capacidad de respuesta ante incidentes de seguridad para las Administraciones Públicas.

En la figura adjunta (129) se muestran estos principios básicos y requisitos mínimos.



Asimismo, en el cuadro adjunto se muestran los diferentes servicios previstos y los organismos responsables de proporcionarlos en el ENS:

(129) RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE nº 25 (29.10.2010).

Se considera, por tanto, que esta norma es un conjunto homogéneo y compacto de medidas de seguridad que, una vez que se apliquen mejorarán considerablemente los niveles de seguridad de los distintos organismos de la Administración.

No obstante, el ENS adolece de algunas deficiencias fruto del consenso en su desarrollo entre la Administración General, Autonómica y Local. Así la revisión de las auditorias y la corrección de las posibles deficiencias detectadas no están supervisadas por ningún organismo que vele porque todas las AAPP mantengan el mismo nivel de seguridad en sus sistemas.

Además, aunque para sistemas de nivel ALTO se establece en las medidas de protección asociadas con la monitorización de sistemas, en el Real Decreto esta actividad no está contemplada con la importancia que sería necesaria para hacer frente a las amenazas actuales.

De todas formas, el esquema en su artículo 29 establece que el CCN elaborará y difundirá guías de seguridad que desarrollen éste. Se espera que estas guías aclaren y subsanen las posibles deficiencias del mismo. En la tabla adjunta se muestra las guías previstas hasta el momento en la serie CCN-STIC 800.

800 – Esquema Nacional de Seguridad	801	Responsabilidades en le ENS
	802	Auditoria del Esquema Nacional de Seguridad
	803	Categorización de los sistemas en el ENS
	804	Implementación de Medias en el ENS
	805	Modelo de política de seguridad
	806	Modelo de Plan de Adecuación al ENS
	807	Criptología de empleo en el ENS
	808	Verificación del cumplimiento de las medidas en el ENS
	809	Declaración de conformidad con el ENS
	810	Guía de Creación de CERT,s
	811	Interconexión en el ENS
	812	Herramientas de seguridad en el ENS

Protección de Datos personales

La Ley Orgánica 15/1999 (130), de 13 de diciembre, de Protección de Datos de Carácter Personal tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas.

Sus normas de desarrollo, determinan las medidas para la protección de los datos de carácter personal y aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

Esta normativa fue la primera de obligado cumplimiento para sistemas dentro de su ámbito de actuación. Normalmente sus medidas de seguridad están asociadas al fichero y no al sistema por lo que la seguridad proporcionada no es integral.

Además de la Agencia Española de Protección de Datos (131), existen en algunas CCAA (Madrid (132), Cataluña (133) o País Vasco (134)) otras agencias con misión similar en su entorno geográfico.

(130) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria)

(131) AEPD Agencia Española de Protección de Datos. www.agpd.es. Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

(132) En Madrid. creada artículo 6 de la Ley 9/1990, de 8 de noviembre, Reguladora de la Hacienda de la Comunidad de Madrid. Estatuto aprobado por el Decreto 40/2004 de 18 de marzo. www.madrid.org/cs/Satellite?language=es&pagename=PortalAPDCM%2FPage%2FPAPD_home

(133) Agencia Catalana de Protección de Datos. www.apdcat.net/ca/index.php

(134) Agencia Vasca de Protección de Datos. www.avpd.euskadi.net/s04-5213/es

Sistemas asociados a Infraestructuras críticas

Actualmente, el anteproyecto de ley asociado a la protección de infraestructuras críticas está en su fase final de aprobación por lo que no se puede determinar el nivel de seguridad de los sistemas asociados a las mismas.

Existen sectores que proporcionan muchos servicios en el ciberespacio y por subsistencia de su negocio implementan unos niveles de seguridad aceptables como puede ser el sector financiero pero existen otros de los que se desconoce realmente el nivel de seguridad que tienen.

Se deberá esperar al desarrollo de esta normativa en el campo de la ciberdefensa para poder valorar realmente el nivel de seguridad de estas infraestructuras.

ESTRATEGIA ESPAÑOLA DE CIBERSEGURIDAD

De lo expuesto en los capítulos 5 y 6 se observa que las responsabilidades en ciberseguridad se encuentran muy disgregadas en diferentes organismos que además no tienen las mismas prioridades desde el punto de vista de seguridad.

Se detecta un posible solape por un lado y una disgregación de funciones por otro que impide un tratamiento completo de los nuevos desafíos de seguridad que nos presenta el ciberespacio.

Por otro lado, y tras analizar cómo se está abordando el problema en otros países de nuestro entorno, se hace necesario desarrollar una estrategia nacional sobre ciberseguridad que trate de forma completa el problema, que permita alcanzar una visión de conjunto sobre el mismo, establezca estructuras que aseguren la coordinación de las iniciativas de cada uno de los organismos con responsabilidades en este ámbito y promueva la adopción de unas líneas estratégicas de acción.

Se describe a continuación una posible aproximación a esta estrategia.

Objetivos

La Estrategia Nacional de Ciberseguridad persigue conseguir un ciberespacio más seguro a través de los siguientes objetivos:

1. Establecer una línea de defensa común y homogénea. Para ello se debe desarrollar con la máxima rapidez el Esquema Nacional de Seguridad y mejorar el intercambio de información de alertas, vulnerabilidades y amenazas que se detecten en las redes de la administración.
2. Mejorar las capacidades de detección y reacción. Para ello se deben mejorar o desarrollar sistemas de alerta temprana e incrementar la seguridad de los productos y tecnologías desde su fase de diseño.
3. Colaborar con la Administración autonómica y local y con el sector privado para apoyar iniciativas que mejoren la seguridad de los sistemas nacionales haciendo especial énfasis en los que gestionan infraestructuras críticas. Extender las acciones de formación y concienciación en ciberseguridad a todos ellos.
4. Concienciar y proporcionar apoyo a los ciudadanos para hacer más segura su actividad en línea (on-line) así como reforzar la capacidad de las fuerzas y cuerpos de seguridad del Estado para combatir el cibercrimen.
5. Fortalecer el entorno futuro de ciberseguridad. Para ello se debe incrementar el número de especialistas en seguridad de las TIC, impulsar y coordinar los esfuerzos de investigación y desarrollo de productos de seguridad nacionales y definir estrategias que disuadan la actividad hostil o dañina en el ciberespacio.

Al igual a lo realizado por otras naciones, para conseguir estos objetivos se deben incrementar los presupuestos de las agencias encargadas de la seguridad de la Administración y las unidades encargadas del ciberdelito en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Líneas estratégicas de acción

Para conseguir estos objetivos se plantean algunas líneas estratégicas que se deben considerar y dotar presupuestariamente:

1. **Desarrollar el Esquema Nacional de Seguridad**, reforzando su aplicación y la realización de auditorías que verifiquen el estado de seguridad de los sistemas de la Administración. El RD no contempla dotación presupuestaria que impulse su aplicación.
2. **Gestión homogénea de las redes de las Administraciones Públicas** minimizando y optimizando sus conexiones a Internet (deben cumplir los mismos requisitos de seguridad) y centralizando las capacidades de Monitorización y respuesta.

3. **Despliegue de sistemas de alerta y protección de las redes de las AAPP y sus interconexiones** para la detección rápida de incidentes y anomalías dentro de éstas. Estos sistemas, basado en el análisis y correlación de registros (logs) generados por las herramientas de seguridad instaladas, permite detectar de manera proactiva cualquier anomalía o ataque analizando el tráfico que circula dentro, entre y en las salidas de los diferentes Ministerios y Organismos.
4. **Desarrollo del Plan de Protección de infraestructuras críticas (PPIC) ante ciberamenazas**. Con el objetivo de gestionar de incidentes de seguridad relacionados con ciberataques sobre infraestructuras críticas; actualizar la información sobre vulnerabilidades (especialmente en sistemas SCADA); impulsar el cumplimiento por parte de los operadores de los estándares de seguridad que se definan como mínimos; realizar análisis de riesgos y ejecutar auditorias de seguridad que revisen el cumplimiento. Sería del máximo interés que estos operadores que manejan infraestructuras críticas se acojan a servicios de alerta temprana similares a los del punto anterior.
5. **Elaborar un programa de concienciación y formación para crear una sólida cultura de seguridad** en el desarrollo y el uso de sistemas de información y comunicaciones a todos los niveles ciudadanos, sector privado (infraestructuras críticas) y Administraciones públicas.
6. **Mejorar los mecanismos de coordinación y respuesta ante incidentes** y realizar ejercicios que demuestren su efectividad. Por ello, se deben crear estructuras de ciberdefensa similares a las de otras naciones en las que se integren las capacidades de respuesta ante incidentes de seguridad existentes actualmente.
7. **Coordinación de esfuerzos en investigación y desarrollo de tecnologías de seguridad** especialmente centrada en el desarrollo de productos de cifra. Se debe evitar el empleo de tecnologías de terceros países en aspectos tan críticos como la protección de la información. En esta acción se debe involucrar al sector privado por su papel en muchas de las infraestructuras críticas nacionales.
8. **Potenciar la colaboración internacional**. Por la naturaleza transnacional de la amenaza y del ciberespacio hace necesario una cooperación internacional para hacerle frente. Se deben impulsar la firma de acuerdos en materia del ciberdelito y crear unas normas

de comportamiento en el ciberespacio consensuadas por todas las naciones que pueda facilitar la atribución de los ataques.

9. **Promover el uso de estándares de seguridad y la certificación de seguridad de los productos TIC**. Es necesario que las tecnologías y productos hayan sido revisadas desde el punto de vista de seguridad. Estos procesos son costosos y difíciles de abordar especialmente para pequeñas y medianas empresas. Esta acción permitiría además, que los productos desarrollados nacionalmente puedan competir en el ámbito internacional.
10. **Mejorar de seguridad en las redes clasificadas**. Estas redes manejan la información clasificada y sensible de la Administración para conducir Operaciones de Mantenimiento de Paz, Operaciones Militares, actividades diplomáticas, actividades contraterroristas, actividades de las FCSE o de inteligencia así como las actividades de seguridad interior. La integridad de estas redes es crítica y cualquier incidente declarado en las mismas puede dañar de forma grave la soberanía nacional. Se debe reforzar por tanto las medidas de seguridad de estos adaptando las salvaguardas y procedimientos existentes a la evolución de los ciberataques.

Se describen con mayor detalle estas posibles líneas de acción en el anexo A.

Posible estructura de la ciberseguridad

Del análisis de las responsabilidades en el ciberespacio se determina que esta actividad está siendo realizada por diferentes Ministerios y se detecta que existen solapes en sus diferentes actividades. Asimismo no están definidos canales de colaboración formales entre las capacidades de respuesta ante incidentes de seguridad.

Por ello, para poder afrontar el reto de la ciberdefensa se considera necesario un organismo (oficina o centro de coordinación) con responsabilidades transversales en este asunto y con una visión global que pueda impulsar todas las líneas de acción.

Puede ser una solución la creación de una **Oficina de Ciberseguridad (OCS)** responsable de desarrollar la política para la defensa cibernética, garantizar su cumplimiento, definir y establecer la estructura funcional necesaria para esta defensa en las Administraciones públicas, apoyar a los operadores privados que gestionen infraestructuras críticas y coordinar las iniciativas de concienciación a los ciudadanos.

Dentro de esta oficina se tiene que articular un organismo de planeamiento que debe ser un órgano colegiado cuyas funciones pueden ser las de implementar y revisar la política de ciberdefensa, revisar las amenazas emergentes con respecto a los planes de defensa e inversiones, revisar las medidas de defensa implementadas en los diferentes organismos, desarrollar el programa de trabajo establecido, aprobar los programas de formación y concienciación y validar y aprobar los informes de evaluación de amenazas, vulnerabilidades y riesgos de seguridad.

Asimismo será necesario disponer de un Centro de Coordinación Técnica en ciberseguridad (CCTCS) con la función principal coordinar las actividades operativas de ciberdefensa de todos los organismos nacionales implicados en la misma, así como con los organismos internacionales que se determinen.

Las misiones de este CCTCS pueden ser:

– Alertar y prevenir los incidentes de seguridad en el ciberespacio y, llegado el caso, responder de forma rápida y eficiente ante cualquier ataque cibernético que se pueda producir.
– Ser punto de contacto para la recepción, valoración y distribución de información de seguridad cibernética.
– Realizar cualquier tipo de coordinación a nivel internacional y ejecutar las acciones necesarias para la mitigación y neutralización de ataques cibernéticos recibidos por otros países.

Dependiendo de CCTCS se deben concentrar las capacidades de respuesta ante incidentes gubernamental en un Centro de Coordinación de Respuesta ante Incidentes de Seguridad (CCRIS).

El ámbito de actuación del CCRIS debe comprender los sistemas clasificados nacionales y aquellos internacionales que por acuerdo o convenio le corresponda proteger al Estado español, los sistemas de la Administración y, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), los sistemas que gestionen infraestructuras críticas.

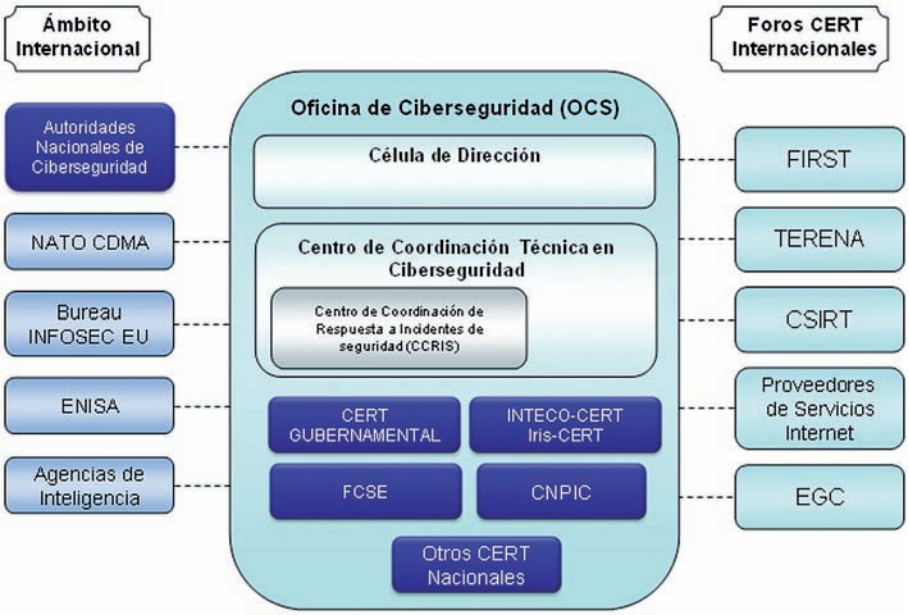
La articulación de una adecuada respuesta ante incidentes en sistemas que gestionan infraestructuras críticas es una actividad crítica que debería realizarse con la mayor celeridad.

El CCRIS debe estar compuesto por representantes del CERT gubernamental, de los distintos CERT,s de ámbito nacional (IRIS-CERT e INTECO-CERT), de los CERT,s autonómicos (CESICAT, CSIRT-CV, Anda-

lucía-CERT), de la Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, del Grupo de Delitos Telemáticos (GDT) de la Guardia Civil, de la División de Investigación Criminal de los Mozos de Escuadra (Mossos d´Esquadra), de la Sección de Delitos Informáticos de la Unidad de Investigación Criminal y Policía Judicial de la Policía Autónoma Vasca (Ertzaintza), de la Unidad Técnica de Policía Judicial de la Guardia Civil entre otros posibles representantes.

No obstante, estará abierto a la adhesión de otros organismos cuando la naturaleza de la amenaza cibernética requiera de su asesoramiento para hacer frente a la misma.

En la figura adjunta se muestran las posibles relaciones de la estructura propuesta.



CONCLUSIONES

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Además no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas.

Todas las naciones de nuestro entorno están desarrollando iniciativas para intentar controlar las amenazas que vienen del ciberespacio. La mayoría de ellas está apostando por estructuras similares a la propuesta en este documento.

En España las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos que abordan el problema de forma parcial.

Es necesario por tanto impulsar actuaciones en este sentido fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante este tipo de amenazas. La dotación presupuestaria se considera crítica si se quieren llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la amenaza.

Por ello, la estrategia propone que se establezca un programa que afecte a todo la nación para alcanzar los objetivos estratégicos planteados incrementando los fondos que desarrollen nuevas tecnologías para proteger las redes nacionales e incrementando la formación en perfiles críticos para esta actividad y fomentando el trabajo coordinado entre el sector público, la industria, los ciudadanos y los aliados internacionales.

BIBLIOGRAFÍA

14th Annual, CSI Computer Crime and Security Survey, diciembre de 2009.

A human capital crisis in cybersecurity. *Technical Proficiency Matters,* Center for Strategic & International Studies, July 2010. [disponible en www.csis.org]

Ataques DDoS 2010. Últimas motivaciones y métodos utilizados, *Informe de Amenazas CCN-CERT IA-05/10,* 10.09.2010, [disponible en www.ccn-cert-cni.es (parte privada del portal)]

CCN-CERT IA-03/10 Ciberamenazas 2009 y Tendencias 2010, *Informe de amenazas del CCN-CERT,* 15 de marzo de 2010, [disponible en www.ccn-cert-cni.es (parte privada del portal)]

Cyber Threats and Trends, *An iDefense® Topical Research Paper,* The VeriSign® iDefense® Intelligence Operations Team, 18 de diciembre de 2009

Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations, Swedish Defense Research Agency (FOI), marzo 2010, [disponible en www2.foi.se/rapp/foir2970.pdf], [consulta 7-10-2010]

ENISA Country Reports, European Network and Information Security Agency (ENISA), enero 2010, [disponible en www.enisa.europa.eu]

International Critical Information Infrastructure Protection Directory, Meridian conference, Issue 24. Spain (page 110), agosto 2010

Jihadist and the Internet. 2009 Update, *National Coordinator for Counterterrorism,* mayo 2010, [disponible en english.nctb.nl/current_topics/reports], [consulta 7-10-2010]

La inteligencia, factor clave frente al terrorismo internacional, Cuadernos de Estrategia nº 141, Ministerio de Defensa, 2009

La Sociedad de la Información en España 2009, *Fundación Telefónica,* 21 de diciembre de 2009, [disponible en e-libros.fundacion.telefonica.com/sie09/aplicacion_sie/ParteA/datos.html y

www.fundacion.telefonica.com/prensa/noticias/noticia.php?prog=debateyconocimiento&noticia=21_12_2009_esp.htm]

MOLINA MATEOS José María, *Aspectos jurídicos de la protección criptológica de la información y las comunicaciones,* Universidad Complutense, Madrid, 1999

Online as soon as it happens, *Informe ENISA*, 8 de febrero de 2010, [disponible en www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens]

PASTOR Oscar, PÉREZ José Antonio, ARNÁIZ Daniel, TABOSO Pedro, *Seguridad Nacional y* Ciberdefensa, Cuadernos Cátedra ISDEFE-UPM, octubre de 2009.

Toward a general policy on the fight against cyber crime, Committee from the Commission to the European Parliament, the Council and the Committee of the Regions, 22 de mayo de 2007

Legislación

Borrador de legislación por el que se establecen medidas para la protección de las infraestructuras críticas. Ministerio del Interior, [disponible en www.cnpic-es.es], [consulta 11-6-2010]

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, *BOE* nº 109 de 7 de mayo de 2002

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, *BOE* nº 150 de 23 de junio de 2007

Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, *BOE* nº 84 de 6 de abril de 1968

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *BOE* nº 298 de 14 de diciembre de 1999

Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, *BOE* nº 230 de 25 de septiembre de 2007

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, *BOE* n. 17 de 19/1/2008

Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, *BOE* nº 52, de 29 de febrero de 1996

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, *BOE* nº 25 de 29 de enero de 2010

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, *BOE* nº 25 de 29 de enero de 2010

Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, *BOE* nº 68 de 19 de marzo de 2004

Reino Unido

CORNISH Paul, HUGHES Rex and LIVINGSTONE David, *Cyberspace and the National Security of the United Kingdom*, Chatham House, March 2009

Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space. Cabinet Office, June 2009, [disponible en www.cabinetoffice.gov.uk]

Estados Unidos

Cybersecurity. Continued Attention is needed to Protect Federal Information Systems from Evolving Threats, United States Government Accountability Office. GAO-10-834T, 16 de junio de 2010, [disponible en www.gao.gov], [consulta 7-10-2010]

Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure, 29 de mayo de 2009, [disponible en www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf], [consulta 7-10-2010]

National Infrastructure Protection Plan, Homeland Security Department, 2006, [disponible en www.dhs.gov], [consulta 7-10-2010]

Privacy Impact Assessment for EINSTEIN 2, United States Computer Emergency Readiness Team (US-CERT), 19 de mayo 2008, [disponible en www.dhs.gov], [consulta 7-10-2010]

The Comprehensive National Cybersecurity Initiative, White House, 2010, [disponible en http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative], [consulta 7-10-2010]

The National Strategy to Secure Cyberspace., White House. Washington

February 2003, [disponible en www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf], [consulta 7-10-2010]

Canadá

Canada's Cyber Security Strategy. For a stronger and more prosperous Canada. 2010, [disponible en www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.aspx], [consulta 7-10-2010]

Estonia

Cyber Security Strategy. Cyber Security Strategy Committee, Ministry of Defence. Estonia, Tallinn 2008, [disponible en [www.mod.gov.ee/en/national-defense-and-society],[consulta 22-10-2010]

Francia

Défense et Sécurité nationale. Le Livre Blanc, Editorial Odile Jacob/ La Documentation Française, junio 2008, [disponible en www.livreblanc-defenseetsecurite.gouv.fr], [consulta 22-10-2010]

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) decreto n° 2009-834 de 7 de julio de 2009, Journal officiel du 8 juillet 2009, [disponible en www.ssi.gouv.fr], [consulta 22-10-2010]

*Plan de Renforcement de la Sécurité des Systèmes d´Information de L'état, m*arzo 2004, [disponible en www.ssi.gouv.fr], [consulta 22-10-2010]

Alemania

Act to Strengthen the Security of Federal Information Technology of 14 August 2009, Act on the Federal Office for Information Security, BSI Act – BSIG, [disponible en www.bsi.bund.de], [consulta 1-10-2010]

Improving IT Security, BSI Annual Report 2008/2009, Federal Office for Information Security BSI, [disponible en www.bsi.bund.de], [consulta 1-10-2010]

National Plan for Information Infrastructure Protection, octubre 2005, [disponible en www.bmi.bund.de], [consulta 1-10-2010]

Australia

Cyber Security Strategy, Attorney General's Department, 23 de noviembre de 2009, [disponible en www.ag.gov.au/cybersecurity], [consulta 7-10-2010]

E-Security Review 2008, Discussion Paper for public consultation, [disponible en www.ag.gov.au/agd/agd.nsf], [consulta 7-10-2010]

Protecting Yourself Online. What Everyone Needs to Know, Australia 2010, [disponible en www.staysmartonline.gov.au], [consulta 7-10-2010]

Security of Infrastructure Control Systems for Water and Transport, Victorian Government Printer, October 2010, [disponible en www.audit.vic.gov.au], [consulta 5-10-2010]

CONCLUSIONES

CONCLUSIONES

POR LUIS JOYANES AGUILAR

La última quincena de noviembre de 2010 ha sido de especial interés y trascendencia para el tema central de nuestra obra dado que se han aprobado sendas iniciativas de la Unión Europea y Estados Unidos de modo conjunto y otra propia de la Unión Europea.

A la terminación de la Cumbre de la OTAN celebrada en noviembre de 2010 en Lisboa la Unión Europea y EE.UU. anunciaron la creación de un grupo de trabajo para combatir los **delitos por internet**, que consideran un problema internacional cada vez mayor. En el comunicado final de la reunión, Washington y Bruselas se declararon comprometidos con la lucha contra los delitos que se comenten por medio de **sistemas informáticos** e internet, considerados también una amenaza en el documento final de la Alianza Atlántica. El grupo de trabajo bilateral euro-estadounidense sobre «ciberseguridad» y «cibercrimen» informará de sus trabajos en el plazo de un año a las dos partes, que destacaron el éxito que han tenido en la negociación de su programa para detectar la financiación del terrorismo.

La Comisión Europea ha propuesto la creación de un Centro Europeo del Cibercrimen para el año 2013 con el objetivo de proteger mejor a ciudadanos y empresas de una nueva forma de delincuencia que, según fuentes de la CE, le cuesta a la UE cada año unos **750.000 millones de euros**. La comisaria de Interior, Cecilia Mamlström (1), ha anunciado la creación del centro contra los **delitos en la Red** que se une a la constitución del grupo de trabajo bilateral UE–Estados Unidos.

(1) Página de Cecilia Malmström, Comisaria de Asuntos de Interior: ec.europa.eu/commission_2010-2014/malmstrom/welcome/default_en.htm y europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1535&format=HTML&aged=0&language=ES&guiLanguage=en [consultado 22 noviembre 2010]

Estas dos buenas noticias en el sector de la ciberseguridad nos sirven de prólogo para la exposición final de las conclusiones de los diferentes capítulos ya citadas con anterioridad y como paso previo a las recomendaciones finales que a modo de Decálogo de intenciones proponemos como conclusión y epílogo final.

ALCANCE Y ÁMBITO DE LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

La ciberseguridad afecta al bienestar digital de la sociedad, de las organizaciones y de los países y, en particular, afecta a distintas dimensiones: política, social, económica, legal, justicia y policial, técnica y de gestión. Los desafíos son complejos y afrontarlos 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 proporcionar confianza y generar un crecimiento del bienestar económico que beneficie a toda la sociedad.

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 planteado algunos países de nuestro entorno (Gran Bretaña, entre ellos) (2)) y en particular la OTAN en la Cumbre de Lisboa celebrada el 20 de noviembre de 2010 y debería constituir el punto de partida de una *Estrategia Nacional de Ciberseguridad,* marco normativo y regulador 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 (3). 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 el conocimiento y las nuevas Tecnologías de la Información y las Comunicaciones deben ayudar a resolver los citados problemas.

---

(2) Véase nota 1 del Capítulo 1.

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

ESTRATEGIAS LEGALES FRENTE A LAS CIBERAMENAZAS

La mutación expansiva de la categoría jurídica de seguridad nacional, que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta un concepto más amplio y multidimensional como es el de seguridad nacional. Este nuevo concepto todavía en formación, no ha acabado de perfilarse con la suficiente concreción jurídica, discurriendo en numerosas ocasiones entre su entendimiento como idea simbólica-emotiva, o como equivalente a interés general identificado con el interés del Estado y contrapuesto al interés individual. Por estas razones el usual manejo del canon de ponderación de intereses para resolver los conflictos entre seguridad nacional y derechos fundamentales, casi siempre se resuelve a favor del primero.

Existe un nuevo escenario estratégico, criminológico y político-criminal, en el que se aprecia no sólo un salto cuantitativo sino también cualitativo. Y en este sentido se habla de una ruptura: los escenarios de ataques son muy variados, con diferentes niveles de riesgo y de muy diversa escala de impacto potencial, lo que complica extraordinariamente su prevención y respuesta estatal. Ahora el *nuevo terrorismo y la nueva criminalidad transnacional*, se muestran con una mayor agresividad y representan un auténtico desafío para los Estados, pero su control, igualmente, hace peligrar los valores del Estado de Derecho, especialmente los derechos fundamentales.

El desarrollo del ciberespacio ha facilitado enormemente el desarrollo de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales. El control de muchos procesos mundiales se realiza a través del ciberespacio que se ha convertido en un bien muy valioso y eso ha hecho que la seguridad del ciberespacio ha crecido en importancia.

A la profesionalización, internacionalización y globalización de la criminalidad, se suma la consolidación del uso de las tecnologías de la información y la comunicación (TIC), Las TIC constituyen instrumentos de alto valor patrimonial, político y estratégico; pero no debe minusvalorarse las facilidades su uso ofrece para la ejecución de ilícitos, lo que a su vez conlleva la generalización y aumento del recurso a estas tecnologías como instrumento comisivo.

Se puede decir que *cibercrimen* y *ciberamenazas* no son categorías equivalentes ya que existen ciberdelitos que no constituyen amenazas a la

seguridad nacional, y no todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética. En los supuestos mencionados –terrorismo y criminalidad organizada–, se considera que determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional.

La combinación de varios de los factores enunciados, ha propiciado el nacimiento o el replanteamiento de una serie de complejas cuestiones jurídicas, tanto relativas a los derechos fundamentales, como a cuestiones penales sustantivas y procesales. En este sentido, la tendencia marcada por el *Convenio sobre Cibercriminalidad*, así como su funcionamiento en general, merece una valoración altamente positiva. El transcurso del tiempo y la constante innovación tecnológica han causado que el Convenio, en ciertas materias, haya quedado parcialmente obsoleto y sería necesario su actualización; este es el caso, a título de ejemplo, de conductas graves no contenidas en el Convenio, como el *phishing*, la suplantación de identidad, o los delitos cometidos en mundos virtuales. Igualmente se hace preciso reforzar y avanzar en materias como la competencia ultraterritorial en cooperación policial internacional.

EL CIBERESPACIO Y EL CRIMEN ORGANIZADO

El delincuente, y en particular el ciberdelincuente, se ha amoldado rápidamente al nuevo escenario que ha supuesto el auge de las nuevas tecnologías y el cambio en las relaciones e interacciones de la sociedad actual frente los usuarios, legisladores y gobiernos que no acaban de vislumbrar la forma de ordenar la pacífica y libre existencia.

La adaptación del ciberdelincuente a este nuevo escenario se ha manifestado en el aprovechamiento de las ventajas de las deficiencias legislativas y del nuevo espacio jurídico. Su adaptación ha sido tal que se ha procurado un espacio de impunidad, que ha supuesto un efecto llamada para la delincuencia. Han desembarcado, de la mano de los expertos informáticos o *hackers,* con toda su fuerza, abriéndose paso las formas más avanzadas de la delincuencia, las bandas organizadas.

Es necesario afrontar con decisión la delincuencia organizada que se manifiesta esencialmente en: el fraude en el comercio electrónico, en la banca electrónica, la figura del Crimen como Servicio (al estilo de los modelos de servicio en la Computación en Nube, Software como Servicio, Infraestructura como Servicio, etc.), las infraestructuras de *mulas* y los muchísimos timos en la Red.

El crimen cibernético es un negocio puro y duro, como se deduce de las declaraciones de Pilar Santamaría (4) en entrevista a *Cinco Días*: «Nosotros 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».

LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN

En el Ciber caso Estonia 2007, la implicación de Rusia y de ciudadanos rusos en los ataques no ofreció ninguna duda a la luz del número de evidencias recolectadas: el tráfico malicioso a menudo contenía elementos de motivación política en lengua rusa, instrucciones precisas de cuándo, cómo y qué atacar fueron diseminadas por números foros, blogs y sitios web rusos.

Pero sin duda los datos más consistente de la implicación de las autoridades rusas en el asunto, si bien no claramente como autores materiales pero sí cómo inductores, colaboradores necesarios o cómplices, son: a) la renuncia por parte del gobierno ruso a acatar el acuerdo de ayuda legal mutua con Estonia, b) la dejación de funciones por parte de las autoridades rusas en el bloqueo durante dos semanas de la embajada estonia en Moscú o en la agresión a la embajadora y c) la presión económica ejercida por Rusia coincidiendo con los ciberataques, evidenciada por el corte de la frontera a transportes pesados procedentes de Estonia, cancelaciones de contratos de importación de productos fabricados en Estonia, cancelación de transportes ferroviarios, como el que unía San Petersburgo con Tallín, etc.

– La amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede afectar a la infraestructura crítica nacional conllevando riesgos de daños físicos para la población.

Un ejemplo claro de esto es el «gusano Stuxnet», un código malicioso que, según los investigadores, es capaz de tomar el control de los sistemas de control automatizados de las fábricas que previamente ha infectado y puede llevar a cabo acciones para las que está programado.

(4) Pilar Santamaría, Directora de Desarrollo de Negocio y Ciberseguridad de Cisco Mediterráneo, en declaraciones a Manuel G. Pascual en *Cinco Días*, 10 de noviembre de 2010, p. 14

– El derecho a disponer de ciber armamento, es un derecho de toda sociedad democrática para poder hacer frente, con los mismos medios, a aquellos que quieren perjudicar sus legítimos intereses.

Otro ciber caso interesante, por ser el primer caso en el que se combinan operaciones militares y operaciones cibernéticas, es el Caso Georgia 2008. Como en el caso Estonia, hay hechos suficientes que inducen a pensar que el gobierno de la Federación Rusa estuvo detrás de la coordinación de las ciber operaciones, pero, a día de hoy, la demostración legal no es posible.

Por todo ello, la OTAN debe hacer un esfuerzo de renovación de acuerdo al tiempo de amenaza al que se enfrenta en la actualidad y al que se enfrentará en el futuro; y eso pasa por considerar el hecho cibernético en:

a) La definición de conceptos, estrategias, doctrinas y procedimientos.
b) En sus formas de actuación
c) En su ámbito de influencia internacional, consolidando colaboraciones y acuerdos entre la OTAN y estados No-OTAN, el sector privado y organizaciones no gubernamentales. La OTAN está en ello.

Evidentemente las consideraciones anteriores encajan plenamente dentro de la Estrategia de Ciberseguridad aprobadas en la cumbre de Lisboa de noviembre de 2010.

LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR

Las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico. La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias.

Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar y aire, a través del ciberespacio.

En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes.

La ciberguerra es asimétrica. El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares.

Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados; tanto su software como su hardware pueden ser saboteados antes de ser unidos en un sistema en explotación. El riesgo de manipulación en el proceso de fabricación es totalmente real y es la menos comprendida de las ciberamenazas. El sabotaje es prácticamente imposible de detectar y peor todavía de erradicar.

A nivel nacional, el Ministerio de Defensa ha llevado a cabo numerosas iniciativas, publicando la Política de Seguridad de la Información, sus normas de aplicación y tomando un buen número de medidas para incrementar la seguridad de su información, tanto en el ámbito de la red de Propósito General como en el de Mando y Control.

La seguridad de la información en el Ministerio de Defensa se estructura en cinco áreas: «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en poder de las empresas», «Seguridad de la Información en las Instalaciones» y «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», designándose Director de Seguridad de la Información del Ministerio al Secretario de Estado de Defensa, y asignándole, en el ámbito del departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas. También se designa al Director General de Infraestructura como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones y en las instalaciones y como órgano de apoyo técnico para la realización de estas tareas, se designa a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa (Inspección General CIS); como

órgano de coordinación de la seguridad de la información del Ministerio, se establece, el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa.

La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio. La seguridad CIS es un campo amplísimo, que requiere de una especialización muy considerable y que además exige que dentro de ella se contemplen a la vez diversos campos de especialización.

La cifra es un aspecto imprescindible de la seguridad de nuestras comunicaciones. El uso masivo de las tecnologías de la información requiere de equipamiento de cifra acorde con las necesidades de los usuarios. Disponer de criptología nacional con seguridad verificable es un principio irrenunciable, ya que poner nuestras comunicaciones en manos de cifradores y algoritmos desconocidos o no controlados en todo su proceso de fabricación es inaceptable. Las tendencias de las nuevas generaciones de equipos de cifra son: interoperabilidad entre cifradores con diferentes redes acceso, interoperabilidad a nivel nacional y con aliados, módulos reprogramables y certificación múltiple.

El mercado de productos de cifra es reducido, limitado casi exclusivamente a la Administración General del Estado y existen pocas empresas nacionales que desarrollen productos cripto, que además son de tamaño y facturación pequeños, por lo que seria necesario un esfuerzo de desarrollo y que éste sea sostenible en el tiempo.

Consideramos que la Unión Europea debería desarrollar una estrategia similar a la contenida en la Iniciativa Nacional de Ciberseguridad de Estados Unidos. En ella se fija el objetivo de establecer estrategias efectivas para blindar las transacciones bancarias y financieras, las redes de transporte por superficie, subterráneas, aéreas y marítimas, y la protección digital de las infraestructuras de comunicaciones civiles y militares, de energía, transporte, seguridad militar, e informática, de toda la nación. Se pretende con evitar que los ciberatacantes provoquen apagones masivos, detengan la actividad comercial y financiera, cometan fraudes a particulares y entidades financieras, o alteren el funcionamiento de las redes de seguridad informáticas civiles y militares.

Esta misma orientación ha tomado la doctrina militar rusa en materia de seguridad en la información, como se ha publicado parcialmente en febrero de 2010 en un documento no clasificado.

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD. CIBERTERRORISMO

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Además no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas

Como ya hemos considerado anteriormente, todas las naciones de nuestro entorno están desarrollando iniciativas para intentar controlar las amenazas que vienen del ciberespacio y la mayoría de ellas está apostando por estructuras similares a la propuesta en el capítulo 6.

En España las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos que abordan el problema de forma parcial.

Es necesario por tanto impulsar actuaciones en este sentido fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante este tipo de amenazas. La dotación presupuestaria se considera crítica si se quieren llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la amenaza.

Por ello, la estrategia propone que se establezca un programa que afecte a todo la nación para alcanzar los objetivos estratégicos planteados incrementando los fondos que desarrollen nuevas tecnologías para proteger las redes nacionales e incrementando la formación en perfiles críticos para esta actividad y fomentando el trabajo coordinado entre el sector público, la industria, los ciudadanos y los aliados internacionales.

PROPUESTAS A MODO DE DECÁLOGO DE LA CIBERSEGURIDAD

Teniendo presentes los análisis y conclusiones realizadas en la ntroducción y los diferentes capítulos de nuestra obra y la aprobación de la Estrategia de Ciberseguridad realizada por la OTAN en la Cumbre de Lisboa del 20 de noviembre de 2010, haremos una propuesta de reflexiones que consideramos fundamentales para el futuro desarrollo de una estrategia de Ciberseguridad Nacional teniendo presentes los retos, oportunidades y amenazas en el contexto de la seguridad nacional;

1. Sería conveniente alcanzar un Sistema Normativo Europeo y Nacional que se adapte con rapidez a la situación cambiante de los riesgos TIC de modo que incluya sanciones para los nuevos delitos provenientes de los ataques informáticos. Las iniciativas de algunos países de nuestro entorno europeo ya examinadas en la obra y la ya citada aprobación de las estrategias de ciberseguridad de la OTAN, pueden ser elementos de apoyo y ayuda a la elaboración del propuesto sistema normativo europeo y nacional.
2. Establecer una plataforma española de ciberseguridad y la posibilidad de crear un Centro Español de la Ciberseguridad dependiente de una Dirección única que actúe de modo centralizado y alineada con las estrategias europeas emanadas de la Agenda Digital Europea (5).
3. Aunar esfuerzos en ciberseguridad a nivel nacional e internacional mediante el intercambio de experiencias y conocimientos. Las experiencias realizadas en Cyber Europe 2010 y las realizadas en España (Ejercicios de Ciberdefensa de las FAS) pueden ser también elementos de referencia,
4. Fomentar la cultura de ciberseguridad en todos los niveles: administración, industria, empresas y ciudadanos (adultos y sobre todo menores).
5. Fomentar la colaboración público-privada en el campo de la seguridad y las infraestructuras críticas, fomentar la modernización tecnológica y en trabajar en aumentar la confianza en los servicios de Seguridad de la Información y las TIC (Tecnologías de la Información y la Comunicación).
6. Fomentar la I+D+i en Seguridad de las TIC (STIC).
7. Alinear los enfoques académicos de seguridad con los nuevos escenarios de amenazas y riesgos TIC.
8. Abogar por una estrategia de ciberseguridad que se traduzca en Sistemas de Gestión de Seguridad de TIC que consideren la Gestión de Riesgos TIC aplicando metodologías pertinentes.
9. Caminar hacia la Gobernanza de las TIC que supone poder gestionarlas adecuadamente, mediante el desarrollo de mecanismos y toma de decisiones que estén alineadas con las prioridades y líneas de las estrategias y control de riesgos TIC.

(5) Acciones clase 7 y otras acciones, en *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*****.** Bruselas, 26.8.2010 COM(2010) 245 final/2. pp. 20-21.

10. La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio y alcanzar una mentalidad de la Ciberseguridad como activo nacional. Para ello las diferentes administraciones debería promover en los planes de estudio de los diferentes escalones educativos la introducción de materias relativas a la ciberseguridad.

Para terminar debemos considerar la necesidad de alineamiento de la estrategia nacional de ciberseguridad con la regulación que en materia de TIC ha aprobado la Unión Europea en su *Agenda Digital para Europa* puesta en marcha en la Declaración de Granada realizada en la reunión de ministros europeos de Telecomunicaciones celebrada en febrero de 2010 en la ciudad de Granada y aprobada y publicada posteriormente.

En particular la Comisión declara en su *acción clave 7* que:

> *«Presentará medidas, incluyendo iniciativas legislativas, para combatir los ciberataques contra los sistemas de información a más tardar en 2010, y una normativa conexa sobre la jurisdicción en el ciberespacio a nivel europeo e internacionala más tardar en 2013» y en otras acciones: «Establecerá una plataforma europea de la ciberdelincuencia a más tardar en 2012» y «Examinará, a más tardar en 2011, la posibilidad de crear un centro europeo de la ciberdelincuencia».*

Entendemos que, el Gobierno de la Nación, como por otra parte ya lo está haciendo, deberá seguir liderando las estrategias en ciberseguridad e iniciar una concienciación y una campaña de educación para promover dicha ciberseguridad.

ANEXO A

LÍNEAS DE ACCIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

LÍNEAS DE ACCIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

JAVIER CANDAU ROMERO

Línea de acción 1: Desarrollo del Esquema Nacional de Seguridad

Como se ha descrito anteriormente el ENS acaba de nacer. Los organismos tienen un plazo de 12 meses, en principio hasta enero de 2011 para su completa implementación.

Se considera que para los sistemas categorizados en nivel ALTO las medidas de seguridad a implementar podrían necesitar a un tiempo de implantación mayor por lo que tras la presentación del correspondiente plan de adecuación, el RD permite una prórroga de hasta 48 meses (enero del 2014).

Este tiempo de aplicación es una muestra del nivel de exigencia que conlleva el cumplimiento del esquema. Además, para cumplir eficazmente muchas de las medidas de seguridad es necesario formar personal especialista, realizar los análisis de riesgos pertinentes, supervisar la implantación de las medidas mediante auditorias, adquirir tecnología o contratar servicios especializados. Por ello su aplicación requerirá una inversión extraordinaria continuada en el tiempo que no está contemplada en la publicación del Real Decreto y que queda bajo responsabilidad de los diferentes organismos.

Sería necesario por tanto, dentro de la estrategia nacional de ciberseguridad, impulsar mediante las dotaciones presupuestarias que se estimen convenientes proyectos que faciliten esta implantación.

Además se deben impulsar programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas.

Línea de acción 2: Gestión homogénea de las redes de las AAPP

Para poder gestionar la amenaza de una manera adecuada se debería realizar una gestión única desde el punto de vista de seguridad de las redes de las AAPP. Las interconexiones con INTERNET deben ser las mínimas posibles y deben cumplir los mismos requisitos de seguridad (este aspecto se trata parcialmente en el ENS).

Actualmente la gestión y la seguridad de las redes corporativas es responsabilidad de cada uno de los Ministerios, CCAA, organismos autónomos y Ayuntamientos. Siendo responsabilidad de cada organismo la seguridad tanto de su red corporativa como de las interconexiones.

Para ello y a través del Consejo Superior de Administración Electrónica, la conferencia sectorial de las AAPP y la conferencia nacional de la Administración local se deben alcanzar unos requisitos mínimos de interconexión que aseguren una defensa homogénea.

Línea de acción 3: Sistemas de protección de las redes de las AAPP

Para garantizar el nivel de seguridad adecuado en los sistemas de las administraciones públicas es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Se debe impulsar la entrada en servicio de sistemas de Alerta Temprana para la detección rápida de incidentes y anomalías dentro de las redes de la Administración. Estos sistemas, basado en el análisis y correlación de registros (logs) generados por las herramientas de seguridad instaladas en las citadas redes, permite detectar de manera proactiva cualquier anomalía y ataque analizando el tráfico que circula en y entre los diferentes Ministerios y Organismos.

Por otro lado es del máximo interés la potenciación de los sistemas similares que permitan monitorizar en tiempo real el tráfico entrante y saliente de las salidas de Internet de los diferentes organismos, recolectando información de seguridad relevante y proporcionando información de los ataques recibidos. Se debe considerar además, la inclusión de los sistemas de las empresas que manejan infraestructuras críticas en estos programas.

Entre otros beneficios, los sistemas de alerta temprana permiten:

– Ofrecer una visión en tiempo real del estado de la seguridad de las redes monitorizadas, relacionando la información proporcionada por los diferentes sensores y disponiendo de estadísticas que permitan medir la eficacia de las medidas de seguridad.
– Disponer de información técnica que permita la implantación de medidas de seguridad adicionales que impidan que ataques similares se vuelvan a reproducir.
– Detección de patrones de ataque comunes a diversas organizaciones que permitan aplicar de forma eficaz medidas de contención y eliminación de los mismos.

La implantación de esta línea de acción será muy costosa en recursos humanos y económicos y su aplicación es muy prolongada en el tiempo, por ello se debe considerar como un servicio horizontal al mayor número de organizaciones posible.

Línea de acción 4: Desarrollo del PPIC ante ciberamenazas

Esta línea de acción se encuentra en su fase inicial pues el borrador de normativa solo lo contempla marginalmente. Sería necesario, por tanto, impulsar la colaboración entre el CNPIC y los organismos especializados en la ciberamenaza en los siguientes campos:

– Gestión de incidentes de seguridad para un tratamiento adecuado de los ciberataques sobre infraestructuras críticas.
– Actualización de información sobre vulnerabilidades tanto de sistemas SCADA como de otros sistemas que soporten estas infraestructuras.
– Cumplimiento por parte de los operadores de los estándares de seguridad que se definan como mínimos.
– Realización de análisis de riesgos y auditorias de seguridad que establezcan los niveles de riesgos a los que están sometidos estos sistemas.

La coordinación debe llevarse a cabo a través de las estructuras que se establezcan al efecto. Sería del máximo interés que estos operadores que manejan infraestructuras críticas se acojan a servicios de alerta temprana similares a los descritos en la línea de acción nº 3.

Línea de acción 5: Programa de formación y concienciación

Según establece la disposición adicional primera del ENS, el personal de las AAPP recibirá la formación necesaria para garantizar el co-

nocimiento de las medidas de seguridad a implementar. Es necesario por tanto un esfuerzo continuado en acciones de formación del personal encargado de su aplicación.

Además serán necesarias acciones de concienciación a todos los usuarios para que conozcan y en la medida de lo posible reduzcan las nuevas amenazas a las que nos enfrentamos y que por su naturaleza cambiante se deben plantear a largo plazo.

Por tanto se deben implicar diversos organismos y se deben desarrollar actividades de formación en seguridad horizontales en los diferentes cursos de acceso a las Administraciones Públicas, programas de sensibilización dirigidos a personal que maneje información sensible o clasificada en sistemas, a usuarios de todas las AAPP que estén implicados en servicios de administración electrónica, a empresas que gestionen infraestructuras criticas con sistemas informáticos que los soporten y especialmente a la alta dirección de los diferentes organismos para que proporcione el apoyo necesario a las actividades de seguridad.

También se debe potenciar el desarrollo de cátedras y jornadas en Universidades y otros centros de formación que traten la seguridad en los sistemas de información y comunicaciones.

Con estas acciones, a largo plazo, se debería construir una cultura de seguridad en el manejo de los sistemas de información que actualmente es prácticamente inexistente en ciudadanos, empresas y administraciones.

Línea de acción 6: Coordinación de recursos en la respuesta ante incidentes de seguridad

El intercambio fluido de información es fundamental para mitigar los daños causados por los ataques desde el ciberespacio al permitir una pronta identificación de éste y la ejecución temprana de una respuesta rápida y adecuada.

Con esta línea de acción se pretende aumentar las capacidades de inteligencia y defensa por ello, se deben mejorar los procedimientos de intercambio de información entre los centros de operación y los centros de respuesta ante incidentes. Es del máximo interés la realización de ejercicios que demuestren la efectividad de estos canales de coordinación.

Esta coordinación se podrá mejorar si se crean estructuras de ciberdefensa similares a las de otras naciones en las que se integren las capacidades de respuesta ante incidentes de seguridad existentes actualmente.

Línea de acción 7: Coordinación de esfuerzos de investigación y desarrollo

Observando la rapidez con la que evolucionan los sistemas, la continua aparición de vulnerabilidades que suponen una amenaza para la integridad de éstos, y la creciente dependencia de la sociedad respecto a las tecnologías de la información, se hace necesario el desarrollo de programas, estrategias y tecnologías que proporcionen unos niveles de seguridad superiores a las que ofrecen los actuales sistemas.

En España, además, una de las deficiencias más importantes que se detectan es la escasez de empresas que desarrollen tecnologías de seguridad. Este vacío, empieza a ser crítico cuando se trata del desarrollo de productos de cifra.

Para poder disponer de autonomía en el empleo de las estas tecnologías es necesario potenciar la coordinación en la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación de productos de seguridad, especialmente si incluyen cifra.

Esta iniciativa se considera crítica para evitar redundancias y para identificar huecos o deficiencias en estos esfuerzos así como para intentar evitar el empleo de tecnologías de terceros países en aspectos tan críticos como la protección de la información.

Es necesario por tanto impulsar el desarrollo de sistemas más seguros, involucrando para ello al sector privado por su papel en muchas de las infraestructuras críticas nacionales.

Línea de acción 8: Potenciar la colaboración internacional

Por la naturaleza transnacional de la amenaza y del ciberespacio hace necesario una cooperación internacional para hacerle frente. Se deben impulsar la firma de acuerdos en materia del ciberdelito y crear unas normas de comportamiento en el ciberespacio consensuadas por todas las naciones que pueda facilitar la atribución de los ataques.

Línea de acción 9: Potenciar el empleo de productos de seguridad certificados

Aunque el ENS contempla que las AAPP valoraran positivamente el empleo de productos que tengan sus funciones de seguridad certificadas, este aspecto no es de obligado cumplimiento para poner cualquier sistema en servicio.

Es necesario que las tecnologías y productos hayan sido revisadas desde el punto de vista de seguridad. Estos procesos son costosos y difíciles de abordar especialmente para pequeñas y medianas empresas. Por tanto se deben impulsar programas que faciliten esta actividad que indudablemente elevará la calidad de los mismos y mejorará la calidad de los productos que consigan esta certificación.

Esta acción permitiría que los productos desarrollados nacionalmente puedan competir en el ámbito internacional pues normalmente poseer una certificación según un estándar internacional (Common Criteria (1) por ejemplo) es requisito imprescindible para poder acceder a cualquier concurso internacional.

Línea de acción 10: Mejoras de seguridad en los sistemas clasificados

Estas redes manejan la información clasificada y sensible de la Administración para conducir Operaciones de Mantenimiento de Paz, Operaciones Militares, actividades diplomáticas, actividades contraterroristas, actividades de las FCSE o de inteligencia así como las actividades de seguridad interior. La integridad de estas redes es crítica y cualquier incidente declarado en las mismas puede dañar de forma grave la soberanía nacional.

Se deben reforzar por tanto las medidas de seguridad de estos adaptando las salvaguardas y procedimientos existentes a la evolución de los ciberataques.

Para ello a través de las estructuras que es establezcan se debería diseñar un plan de mejora de las mismas y potenciar las capacidades de los organismos que deben auditar y monitorizar la actividad de estas redes.

(1) Common Criteria. www.commoncriteria.org

ANEXO B

GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

ANEXO B
GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

Acrónimo / voz	*Significado*
Amenaza (Threat) (OTAN)	La posibilidad de compromiso, pérdida o robo de información clasificada OTAN o de servicios y recursos que la soportan. Una amenaza puede ser definida por su origen, motivación o resultado y puede ser deliberada o accidental, violenta o subrepticia, externa o interna.
ANS	Autoridad Nacional de Ciberdefensa
Bot Botnet	Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación [distribuida] de servicio.
Brecha de seguridad (Security breach) (OTAN)	Una acción u omisión, deliberada o accidental, contraria a la Política de Seguridad de la OTAN o normativas de aplicación de la Política que resulte en un compromiso real o potencial de información clasificada OTAN o los servicios y recursos que la soportan.
Caballo de Troya	Ver troyano
CACD	Centro Asesor para la ciberdefensa (CACD)
Carding	Uso ilegítimo de las tarjetas de crédito.
Catálogo Nacional de Infraestructuras Estratégicas	La información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.
CCC	Centro de Coordinación de Ciberdefensa.
CCN	Centro Criptológico Nacional

CCRIS	Centro de coordinación y respuesta a incidentes de Seguridad
CERT	Computer Emergency Response Team
Ciberataque	Forma de ciberguerra / ciberterrorismo donde combinado con un ataque físico o no se intenta impedir el empleo de los sistemas de información del adversario o el acceso la misma
Ciberdefensa	La aplicación de medidas de seguridad para proteger las los diferentes componentes de los sistemas de información y comunicaciones de un ciberataque.
Ciberespacio (Cyber space) (OTAN)	El mundo digital generado por ordenadores y redes de ordenadores, en el cual personas y ordenadores coexisten y el cual incluye todos los aspectos de la actividad «online».
Ciberevento (Cyber event) (OTAN)	Cualquier suceso observable en un sistema de información y comunicaciones.
Ciberincidente (Cyber incident) (OTAN)	Ciberevento adverso en un sistema de información y comunicaciones o la amenaza de que se produzca.
Ciberseguridad	Protección de los componentes de las infraestructuras de los sistemas de información y comunicaciones ante amenazas cibernéticas
Ciberterrorismo	Un ciberataque para causar la inutilización o interrupción de redes de ordenadores o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico
Código dañino o malicioso (malicious code o software)	Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. [http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]
EGC	*European Government CERT*
Exploit	Pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado).
FIRST	Forum for Incident Response and Security Teams

Gestión de Riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
Gestión del riesgo (Risk Management) (OTAN)	Aproximación sistemática, basada en la valoración de las amenazas y las vulnerabilidades, para la determinación de las contra-medidas necesarias para la protección de la información o los servicios y recursos que la soportan.
Información (Information) (OTAN)	Conocimiento que puede ser comunicado de cualquier forma.
Información clasificada (Classified information) (OTAN)	Información o materia determinada que requiere protección contra revelación no autorizada y a la que, consecuentemente, se le ha asignado un grado de clasificación de seguridad.
Infraestructuras críticas (IC)	Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales
Infraestructuras críticas europeas (ICE)	Aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya interrupción o destrucción afectarían gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114/CE.
Infraestructuras estratégicas (IE)	Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios públicos esenciales
INTECO	*Instituto Nacional de Tecnologías de la Comunicación.*
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
Interdependencia	Los efectos que una interrupción en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y/o en otros sectores, y las repercusiones de ámbito local, regional, nacional o internacional.
OTAN	*North Atlantic Treaty Organization* Organización del Tratado del Atlántico Norte

Phishing	Los ataques de «phishing» usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura («spam») para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc. *[http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]*
RAT	*Remote Administrations Tool.* Herramienta de administración remota. Estas apliaciones pueden ser legítimas o no y pueden ser utilizadas con o sin autorización del usuario. En el mundo del malware estas aplicaciones generalmente son troyanos que abren una puerta trasera (backdoor) en el equipo del usuario para permitir dicha administración.
RAT (2)	*Troyano de Acceso Remoto.* Son programas de software malintencionados que permiten a los delincuentes controlar un equipo mediante la conexión a Internet. Un RAT puede permitir a un delincuente ver y cambiar los archivos y funciones del equipo, supervisar y registrar sus actividades y utilizar su equipo para atacar a otros.
Riesgo (Risk) (OTAN)	La probabilidad de que una vulnerabilidad sea explotada con éxito por una amenaza produciendo un compromiso de confidencialidad, integridad y/o disponibilidad y daños.
Rootkit	Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos. *[http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]*

SCADA	Supervisory Control And Data Acquisition Control Supervisor y Adquisición de Datos, nombre de los sistemas de control industrial.
Sistema de Información	Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
Spam	*Correo basura* Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de usuarios están expuestos a este correo basura, más del 80% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet. *[http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]*
Spyware	Código dañino diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario. [STIC-400:2006]
STIC	Seguridad de las Tecnologías de Información y Comunicaciones.
TERENA	*Trans-European Research and Education Networking Association* Grupo de coordinación de CERT,s europeos
TF-CSIRT (TERENA)	Trans-European Research and Education Network Association
Troyano – Caballo de Troya	Introducción subrepticia en un medio no propicio, con el fin de lograr un determinado objetivo. Diccionario de la Lengua Española. Vigésimo segunda edición. 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. [STIC-430:2006]

Vulnerabilidad (Vulnerability) (OTAN)	Una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada OTAN o los servicios y recursos que la soportan.
Vulnerabilidad	Una debilidad que puede ser aprovechada por una amenaza.
Zombi	Ver bot / botnet

COMPOSICIÓN DEL GRUPO DE TRABAJO

Coordinador:

D. LUIS JOYANES AGUILAR
Catedrático de Lenguajes y Sistemas Informáticos
Escuela Superior de Ingeniería y Arquitectura
Universidad Pontificia de Salamanca

Vocal y Secretaria:

Dª. MARIA JOSE CARO BEJARANO
Licenciada en Informática
Analista principal
Instituto Español de Estudios Estratégicos

Vocales:

D. JOSÉ LUIS GONZÁLEZ CUSSAC
Catedrático de Derecho Penal
Universidad de Valencia

D. JUAN SALOM CLOTET
Comandante de la Guardia Civil
Diplomado de Informática del Ejército
Unidad Central Operativa – Grupo de Delitos Telemáticos

D. NESTOR GANUZA ARTILES
Teniente Coronel de Transmisiones. Ejército de Tierra
Centro de Ciberdefensa de la OTAN en Tallin-Estonia

D. JUAN DÍAZ DEL RÍO DURÁN
Capitán de Navío
Jefe de la Sección de Seguridad de la Información de la División CIS del EMACON

D. JAVIER CANDAU ROMERO
Teniente Coronel de Artillería
Jefe del Área de Políticas y Servicios
Centro Criptológico Nacional

ÍNDICE

Página

CUADERNOS DE ESTRATEGIA

Nº	TÍTULO
*01	La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica.
*02	La ingeniería militar de España ante el reto de la investigación y el desarrollo en la Defensa Nacional.
*03	La industria española de interés para la defensa ante la entrada en vigor del Acta Única.
*04	Túnez: su realidad y su influencia en el entorno internacional.
*05	La Unión Europea Occidental (UEO) (1955-1988).
*06	Estrategia regional en el Mediterráneo Occidental.
*07	Los transportes en la raya de Portugal.
*08	Estado actual y evaluación económica del triángulo España-Portugal-Marruecos.
*09	Perestroika y nacionalismos periféricos en la Unión Soviética.
*10	El escenario espacial en la batalla del año 2000 (I).
*11	La gestión de los programas de tecnologías avanzadas.
*12	El escenario espacial en la batalla del año 2000 (II).
*13	Cobertura de la demanda tecnológica derivada de las necesidades de la Defensa Nacional.
*14	Ideas y tendencias en la economía internacional y española.
*15	Identidad y solidaridad nacional.
*16	Implicaciones económicas del Acta Única 1992.
*17	Investigación de fenómenos belígenos: Método analítico factorial.
*18	Las telecomunicaciones en Europa, en la década de los años 90.
*19	La profesión militar desde la perspectiva social y ética.
*20	El equilibrio de fuerzas en el espacio sur europeo y mediterráneo.
*21	Efectos económicos de la unificación alemana y sus implicaciones estratégicas.

*22 La política española de armamento ante la nueva situación internacional.

*23 Estrategia finisecular española: México y Centroamérica.

*24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas).

*25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida.

*26 Estrategia en el área iberoamericana del Atlántico Sur.

*27 El espacio económico europeo. Fin de la guerra fría.

*28 Sistemas ofensivos y defensivos del espacio (I).

*29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT).

*30 La configuración de Europa en el umbral del siglo xxi.

*31 Estudio de "inteligencia operacional".

*32 Cambios y evolución de los hábitos alimenticios de la población española.

*33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE.

*34 La energía y el medio ambiente.

*35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas defensa.

*36 La evolución de la seguridad europea en la década de los 90.

*37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990.

*38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas.

*39 Las fronteras del Mundo Hispánico.

*40 Los transportes y la barrera pirenaica.

*41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX.

*42 Las expectativas de la I+D de Defensa en el nuevo marco estratégico.

*43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III).

*44 Sistemas ofensivos y defensivos del espacio (II).

*45 Desequilibrios militares en el Mediterráneo Occidental.

*46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa.

*47 Factores de riesgo en el área mediterránea.

*48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990).

*49 Factores de la estructura de seguridad europea.

*50 Algunos aspectos del régimen jurídico-económico de las FAS.

*51 Los transportes combinados.

*52 Presente y futuro de la Conciencia Nacional.

*53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa.

*54 Evolución y cambio del este europeo.

*55 Iberoamérica desde su propio sur (La extensión del Acuerdo de Libre Comercio a Sudamérica).

*56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos.

57 Simulación en las Fuerzas Armadas españolas, presente y futuro.

*58 La sociedad y la Defensa Civil.

*59 Aportación de España en las Cumbres Iberoamericanas: Guadalajara 1991-Madrid 1992.

*60 Presente y futuro de la política de armamentos y la I+D en España.

61 El Consejo de Seguridad y la crisis de los países del Este.

*62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas.

Nº	TÍTULO
63	Los grandes maestros de la estrategia nuclear y espacial.
*64	Gasto militar y crecimiento económico. Aproximación al caso español.
*65	El futuro de la Comunidad Iberoamericana después del V Centenario.
*66	Los estudios estratégicos en España.
*67	Tecnologías de doble uso en la industria de la defensa.
*68	Aportación sociológica de la sociedad española a la Defensa Nacional.
*69	Análisis factorial de las causas que originan conflictos bélicos.
*70	Las conversaciones internacionales Norte-Sur sobre los problemas del Mediterráneo Occidental.
*71	Integración de la red ferroviaria de la península Ibérica en el resto de la red europea.
*72	El equilibrio aeronaval en el área mediterránea. Zonas de irradiación de poder.
*73	Evolución del conflicto de Bosnia (1992-1993).
*74	El entorno internacional de la Comunidad Iberoamericana.
*75	Gasto militar e industrialización.
*76	Obtención de los medios de defensa ante el entorno cambiante.
*77	La Política Exterior y de Seguridad Común (PESC) de la Unión Europea (UE).
*78	La red de carreteras en la penísula Ibérica, conexión con el resto de Europa mediante un sistema integrado de transportes.
*79	El derecho de intervención en los conflictos.
*80	Dependencias y vulnerabilidades de la economía española: su relación con la Defensa Nacional.
*81	La cooperación europea en las empresas de interés de la defensa.
*82	Los cascos azules en el conflicto de la ex Yugoslavia.
83	El sistema nacional de transportes en el escenario europeo al inicio-del siglo xxi.

*84 El embargo y el bloqueo como formas de actuación de la comunidad internacional en los conflictos.

*85 La Política Exterior y de Seguridad Común (PESC) para Europa en el marco del Tratado de no Proliferación de Armas Nucleares (TNP).

86 Estrategia y futuro: la paz y seguridad en la Comunidad Iberoamericana.

87 Sistema de información para la gestión de los transportes.

*88 El mar en la defensa económica de España.

*89 Fuerzas Armadas y Sociedad Civil. Conflicto de valores.

*90 Participación española en las fuerzas multinacionales.

*91 Ceuta y Melilla en las relaciones de España y Marruecos.

92 Balance de las Primeras Cumbres Iberoamericanas.

*93 La cooperación Hispano-Franco-Italiana en el marco de la PESC.

*94 Consideraciones sobre los estatutos de las Fuerzas Armadas en actividades internacionales.

95 La unión económica y monetaria: sus implicaciones.

96 Panorama estratégico 1997/98.

97 Las nuevas españas del 98.

*98 Profesionalización de las Fuerzas Armadas: los problemas sociales.

99 Las ideas estratégicas para el inicio del tercer milenio.

100 Panorama estratégico 1998/99.

*100 1998/99 Strategic Panorama.

101 La seguridad europea y Rusia.

102 La recuperación de la memoria histórica: el nuevo modelo de democracia en Iberoamérica y España al cabo del siglo XX.

*103 La economía de los países del norte de África: potencialidades y debilidades en el momento actual.

104 La profesionalización de las Fuerzas Armadas.

105 Claves del pensamiento para la construcción de Europa.

106 Magreb: percepción española de la estabilidad en el Mediterráneo, prospectiva hacia el 2010.

106-B Maghreb: percepción espagnole de la stabilité en Méditerranée, prospective en vue de L'année 2010

*107 Panorama estratégico 1999/2000

*107 1999/2000 Strategic Panorama.

108 Hacia un nuevo orden de seguridad en Europa.

109 Iberoamérica, análisis prospectivo de las políticas de defensa en curso.

110 El concepto estratégico de la OTAN: un punto de vista español.

111 Ideas sobre prevención de conflitos.

112 Panorama Estratégico 2000/2001.

*112-B Strategic Panorama 2000/2001.

113 Diálogo Mediterráneo. Percepción española.

*113-B Le dialogue Méditerranéen. Une perception espagnole.

114 Apartaciones a la relación sociedad - Fuerzas Armadas en Iberoamérica.

115 La paz, un orden de seguridad, de libertad y de justicia.

116 El marco jurídico de las misiones de las Fuerzas Armadas en tiempo de paz.

117 Panorama Estratégico 2001/2002.

*117-B 2001/2002 Strategic Panorama.

118 Análisis, Estrategia y Prospectiva de la Comunidad Iberoamericana.

119 Seguridad y defensa en los medios de comunicación social.

120 Nuevos riesgos para la sociedad del futuro.

121 La industria europea de defensa: Presente y futuro.

122 La energía en el espacio Euromediterráneo.

*122-B L'énergie sur la scène euroméditerranéenne.

123 Presente y futuro de las relaciones cívico-militares en Hispanoamérica.

124 Nihilismo y terrorismo.

125 El Mediterráneo en el nuevo entorno estratégico.

*125-B The mediterranean in the new strategic environment.

126 Valores, principios y seguridad en la comunidad iberoamericana de naciones.

127 Estudios sobre inteligencia: fundamentos para la seguridad internacional.

128 Comentarios de estrategia y política militar.

129 La seguridad y la defensa de la Unión Europea: retos y oportunidades.

*130 El papel de la inteligencia ante los retos de la Seguridad y Defensa Internacional.

131 Crisis locales y Seguridad Internacional: El caso Haitiano.

132 Turquía a las puertas de Europa.

133 Lucha contra el terrorismo y derecho internacional.

134 Seguridad y defensa en Europa. Implicaciones estratégicas.

*135 La seguridad de la Unión Europea: nuevos factores de crisis.

136 Iberoamérica: nuevas coordenadas, nuevas oportunidades, gandes desafíos.

137 Iran, potencia emergente en Oriente Medio. Implicaciones en las estabilidad del Mediterráno.

138 La reforma del sector de seguridad: el nexo entre la seguridad, el desarrollo y el buen gobierno.

139 Security sector reform: the connection between security, development and good governance.

140 Impacto de los riesgos emergentes en la seguridad marítima.

141 La inteligencia, factor clave frente al terrorismo internacional.

142 Del desencuentro entre culturas a la Alianza de Civilizaciones. Nuevas aportaciones para la seguridad en el Mediterráneo

143 El auge de Asia: implicaciones estratégicas.

144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad.

144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad.

145 La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa.

145 B The European Security and Defense Policy (ESDP) after the entry into Force of the Lisbon Treaty.

146 Respuesta Europea y Africana a los problemas de seguridad en África.

146 B European and African response to security problems in Africa.

147 Los actores no estatales y la seguridad internacional: su papel en la resolución de conflictos y crisis.

148 Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción.

* Agotado. Disponible en las bibliotecas especializadas y en el Centro de Documentación del Ministerio de Defensa.