MAYO 2015 / Nº 3

# CIBER elcano

REAL INSTITUTO elcano ROYAL INSTITUTE

Desarrollado por:

THIBER

INFORME MENSUAL DE CIBERSEGURIDAD

## Copyright y derechos:

**Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos-THIBER, the Cyber Security Think Tank**

Todos los derechos de esta Obra están reservados a Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos y a THIBER, the Cyber Security Think Tank. Los titulares reconocen el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

a) Que se reconozca la propiedad de la Obra indicando expresamente los titulares del Copyright.
b) No se utilice con fines comerciales.
c) No se creen obras derivadas por alteración, trasformación y/o desarrollo de esta Obra.

Los titulares del Copyright no garantizan que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados.

Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Obra son de propiedad exclusiva de los titulares correspondientes.

Más información:

**Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.**

**THIBER, The Cyber Security Think Tank**

# Índice

1 Comentario Ciberelcano ..... 04

2 Análisis de actualidad internacional ..... 07

3 Entrevista a Fco. Javier García Carmona ..... 14

4 Informes y análisis sobre ciberseguridad publicados en abril 2015 ..... 18

5 Herramientas del analista ..... 19

6 Análisis de los ciberataques del mes de abril de 2015 ..... 21

7 Recomendaciones

7.1 Libros y películas ..... 25

7.2 Webs recomendadas ..... 27

7.3 Cuentas de Twitter ..... 27

8 Eventos ..... 28

# 1 COMENTARIO CIBERELCANO.
## La nueva estrategia ciber del Pentágono: innovar y potenciar la industria

**AUTORES:**
**Enrique Fojón Chamorro. Subdirector de THIBER, the cybersecurity Think Tank.**

(Ashton Carter, secretario de Defensa de EEUU, en la conferencia del pasado 23 de abril en la Universidad de Stanford / *U.S. Department of Defense*)

El pasado 23 de Abril, el Secretario de Defensa estadounidense Ashton Carter cerraba su importante visita a Silicon Valley –donde tienen su sede las principales empresas tecnológicas del país– con una conferencia en la Universidad de Stanford bajo el evocador título: *'Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity'*. Durante la misma, Carter argumentó la obligada necesidad del Departamento de Defensa (DoD) para estar a la vanguardia de la innovación tecnológica –como elemento central de la *tercera estrategia de compensación (Third Offset Strategy)* presentada durante el pasado mes de octubre- y , en este sentido, definió las líneas maestras de la *The DoD Cyber Strategy* que se publicó este mismo día.

Esta nueva estrategia, de marcado carácter disuasorio, explica los principales riesgos y amenazas a los que se enfrenta el DoD –y por extensión el gobierno y los ciudadanos estadounidenses– en el ciberespacio; identifica claramente los organismos y personas responsables de implementar esta estrategia, así como el modo en el que se va a implementar; las principales medidas que se van a adoptar y los objetivos que se ha marcado el Pentágono hasta 2018.

En este sentido, los aspectos más relevantes de esta estrategia son los siguientes:

Se trata del primer documento de estas características en afirmar que **Washington podrá utilizar la ciberguerra como una opción en los conflictos futuros**, al afirmar que Estados Unidos "…debe ser capaz de utilizar las ciberoperaciones para disrumpir las redes de mando y control, infraestructuras críticas y sistemas de armas de los potenciales adversarios del país."

Las **ciberoperaciones se integrarán plenamente en el planeamiento y conducción de las operaciones militares**, para ello, ademas de **potenciar la construcción de cibercapacidades a nivel conjunto**, el Pentágono ha planificado crear una ciberfuerza compuesta por 6.200 efectivos repartidos en *DoD Three Primary Cyber Missions* cuyas tareas principales están relacionadas con la defensa, inteligencia y ataque. Estos equipos no estarán formados únicamente por personal militar, sino también por personal civil y reservistas, a tiempo parcial.

En línea con *las lecciones aprendidas de la Revolución en los Asuntos Militares (RMA)* y *el proceso de Transformación de la Defensa*, el Pentágono hace años que ha comprendido que la innovación tecnológica ya no tiene como motor principal al entono militar. En este sentido, aunque el DoD seguirá financiando –bien vía la tradicional Agencia de Proyectos Avanzados (DARPA, en sus siglas en inglés) o mediante la Iniciativa de Innovación en Defensa– proyectos tecnológicos de primer nivel que luego tendrán su aplicación directa en la vida de los ciudadanos, cada vez más la financiación privada es la que nutre este desarrollo tecnológico.

En este sentido, la visita de Carter a Silicon Valley tiene un claro mensaje: **el Departamento de Defensa necesita una industria tecnológica siempre a la vanguardia, en especial, en el ámbito de la ciberseguridad y la ciberdefensa.** Para ello, el DoD va a poner sobre la mesa miles de millones de dólares para dinamizar y evolucionar la industria tecnológica en el ámbito militar. En este sentido, creará la Defense Innovative Unit Experimental con la misión de fortalecer las relaciones entre las empresas tecnológicas y el Pentágono, estar al día de las nuevas tecnologías y ayudar a las nuevas start-ups a iniciar su relación con el DoD sin perderse en la inmensidad burocrática de Washington. Además, financiara nuevos proyectos a través de *IN-Q-Tel*, una entidad de capital riesgo financiada por la CIA que identifica e invierte en empresas que desarrollan tecnologías de vanguardia útiles para la seguridad nacional, y que lleva más de 15 años trabajando en Silicon Valley.

*"el Departamento de Defensa necesita una industria tecnológica siempre a la vanguardia"*

La nueva estrategia establece la **creación de la Oficina del Asesor Principal en materia de Ciberdefensa del Secretario de Defensa** que interactuara con el DoD a través de un consejo de administración e inversión cibernética (CIMB), cuyo objetivo principal es coordinar y sincronizar todos los programas y actividades en materia de ciber que se desarrollen desde el Pentágono, sin interferir en la cadena de mando. Además, el CIMB estará asesorado por un grupo de expertos de primer nivel.

Por último, pero no menos importante, se prevé llevar a cabo una **gestión eficiente de los presupuestos que el DoD destina a actividades ciber**. Este presupuesto está muy repartido entre los diferentes organismos del Pentágono, siendo altamente ineficiente su gestión y uso.

En resumen, con independencia de las líneas maestras establecidas en materia estratégico-militar por la nueva estrategia ciber del Pentágono, puede que el elemento más relevante de la misma sea que el DoD ha descubierto que el primer –y quizás el único– paso para seguir manteniendo la supremacía militar y seguir siendo la primera potencia mundial en materia cibernética pasa por **dinamizar, potenciar y consolidar la industria nacional de ciberseguridad**. Sólo así el Departamento de Defensa y sus Fuerzas Armadas podrán disponer de los medios, capacidades y conocimientos necesarios para mantener el liderazgo en el ciberespacio.

# 2 ANALISIS DE ACTUALIDAD INTERNACIONAL:
## El avance de la ciber-retorsión

**AUTORES: Ángel Vallejo, Responsable de relaciones institucionales de THIBER. Socio Maio Legal.**
**Modesto Abad, Abogado Maio Legal.**

Tras catorce meses de investigación por la Unidad de Investigación Tecnológica de la Comisaría General de Policía Judicial (UIT), el presidente de un grupo de comunicación en España fue imputado por un juzgado de instrucción de Madrid, que anticipa un delito continuado de daños informáticos del artículo 264 del Código Penal (CP), tras repetidos ataques de denegación de servicio distribuido o DDoS (Distributed Denial of Service), a la página web de un medio digital competidor del primero, motivado al parecer por una "venganza" frente a las informaciones publicadas por dicho medio sobre la crisis económica que atravesaba el anterior.

En Estados Unidos, el banco JP MORGAN CHASE sufrió en verano de 2014 un ciberataque que causó preocupación no solo en el entorno de Wall Street, sino en las más altas instancias políticas norteamericanas. Cuando se supo que el incidente tuvo lugar a pesar de que banco venía invirtiendo una media anual de 250 M $ en mejorar su ciberseguridad, la sensación de que se estaba cruzando *la delgada línea roja* llegó hasta la Casa Blanca.

No mucho más lejos, la compañía SONY PICTURES ENTERTAINMENT (SONY) sufrió a finales de 2014 un ataque aparentemente ejecutado por ciberactores norcoreanos. Las autoridades norcoreanas manifestaron que varias de sus instituciones habrían sido, a su vez, atacadas por ciberactores norteamericanos.

Estas noticias ponen sobre la mesa cuestiones que resultan de indudable relevancia en el marco de las Tecnologías de la Información y las Comunicaciones (TIC). En el primero de los casos, el tiempo transcurrido entre los ataques y la imputación formal de los mismos a personas determinadas fue de más de un año. En el caso de SONY, por motivos de extraterritorialidad, entre otras cosas, no ha habido de momento una imputación formal, algo similar a lo que ocurre con el JP MORGAN CHASE.

En el tiempo que transcurre entre un cibertataque y la atribución del mismo (si es que ésta llega a hacerse) la víctima puede permanecer expuesta a un riesgo continuo, y para gestionarlo debe plantearse si adopta una postura activa o pasiva.

En el caso del medio digital español atacado, la brecha temporal entre el ataque y la actuación efectiva de la justicia resulta inadmisible porque el aparato del Estado tardó demasiado tiempo en auxiliar a la víctima y localizar al presunto agresor. De aquí surgen significativos interrogantes que no tienen pronta respuesta. Si las autoridades no logran actuar con rapidez ¿debe permanecer la víctima en actitud pasiva ante graves agresiones perpetradas usando

las TIC como instrumento y vía? ¿Es lícito que el atacado pase a contraatacar a su agresor para defenderse de un ciberataque?

## ¿Pueden los Estados proteger hoy a sus ciudadanos de los ciberataques?

La gran variedad de formas en las que puede materializarse un ciberataque, el origen y alcance global que pueden tener este tipo de ofensivas, así como la enorme dificultad que existe para identificar al verdadero culpable del ataque (el ya paradigmático *attribution issue*), son factores que hacen que, si la seguridad total es una quimera en cualquier ámbito, en el ciberespacio se torne una meta inalcanzable. Michael Daniel, coordinador de ciberseguridad de la Casa Blanca (el conocido como Ciber-Zar norteamericano) es muy gráfico en la expresión de tal problema: *"La atribución es muy complicada. Los malos no suelen usar equipos con etiquetas que rezan <<servidor de los malos>>"*

El perfil de alguna de las víctimas de los más sonados ciberataques arroja elementos para la preocupación. La red eléctrica de la costa este de Estados Unidos y Canadá en el verano de 2003 sufrió un apagón que dejó sin luz a ciudades como Nueva York o Toronto durante días. El Pentágono sufrió el 21 de abril de 2009 el robo de información sensible del caza de quinta generación *Joint Strike Fighter F-35 Lightning II*. La citada SONY vio dañado parte de sus activos digitales por causa del mencionado ciberataque presuntamente perpetrado desde Pyongyang, como respuesta, se dice, al estreno de la película "The Interview", que parodia al líder de Corea del Norte, Kim Jong-Un.

Todas son instituciones de primer nivel, tecnológicamente muy avanzadas, que invierten una buena parte de su presupuesto anual en seguridad e I+D+i. Aun así, son objeto de ciberataques cada vez más sofisticados, devastadores y difíciles de rastrear.

A la luz de estos hechos y de las características de los atacados se puede afirmar que los Estados, que en ocasiones cuentan hoy con menos recursos que alguna de las víctimas antes referidas, no están en condiciones de prevenir o repeler los ciberataques que sufran sus infraestructuras, instituciones, organismos, empresas clave o ciudadanos.

Desde luego en España la situación no es halagüeña. La conclusión no es distinta en países mucho más avanzados que el nuestro en ciberdefensa, como Estados Unidos, China o Israel. Los ejemplos de ataque antes señalados avalan esta conclusión. ¿Qué pueden hacer las víctimas en esta situación?

## *Hacking back:* La ciber-retorsión como elemento de defensa y recuperación.

Hay que enfocar la cuestión desde el punto de vista de política jurídica, porque esa suerte de contraataque del propio perjudicado presenta ciertas dudas conceptuales que hoy día no están despejadas por las normas de los países de nuestro ámbito de relación tecnológico y cultural.

Muchos son los enfoques que han tratado tradicionalmente la cuestión de la autodefensa. Por un lado y con carácter general, un punto de partida teórico podría ser el del sistema de derecho internacional público (DIP), que cuenta con la figura de la *"retorsión"*. Una de las acepciones que el Diccionario de la Real Academia Lengua ofrece es el de *"Acción de devolver o inferir a alguien el mismo daño o agravio que de él se ha recibido"*.

La retorsión está comúnmente aceptada en el DIP, que la identifica con los actos lícitos, pero hostiles, que un Estado realiza contra otro en respuesta a un previo acto de igual naturaleza (incluso ilícito) realizado previamente por éste último contra aquél. Son ejemplos de retorsión la ruptura de relaciones diplomáticas y la restricción de los visados de entrada en el país. Sin embargo, lo que es predicable de los Estados, resulta comúnmente poco extrapolable a los individuos (sean personas físicas o compañías). España comparte con una buena parte de países el principio del monopolio de las estructuras estatales en el uso de la fuerza. El problema surge cuando, como ocurre en el nivel cibernético no estatal al que nos referimos, el concepto es el potencial uso de la fuerza por individuos que no ostentan la representación del Estado ni pertenecen a sus fuerzas y cuerpos de seguridad.

Las soluciones que se vienen discutiendo distan de ser pacíficas en su entendimiento, si bien comparten un aparente principio de rechazo a legitimar los conocidos como *"retaliatory ciberatacks"*. Este rechazo formal, sin embargo, no debe puede hacernos olvidar que, de facto, las actividades de ciber-retorsión se producen continuamente.

Los casos de SONY y el JP MORGAN CHASE han servido para reactivar el debate. El hecho de que el presidente Obama comentara públicamente el caso SONY permitió constatar que el tema se consideraba relevante: *"Responderemos de manera proporcional, en el modo, lugar y tiempo que elijamos. No podemos tener una sociedad en la que un dictador pueda empezar a imponer la censura en Estados Unidos".*

La guerra terminológica se activó de manera inmediata y, según quien expusiera su visión, podía hablarse de *"defensa activa" (active defense)*, de *"contra hackeo" (hackback)*, o de ataque en retorsión o ciber-retorsión *(retaliatory ciberatack)*. Los movimientos de imagen y opinión pública de los lobbies más relevantes, que clamaban por una suerte de derecho a la ciber-defensa propia, generaron como efecto directo la invocación de la ilegalidad del *hackback* y de los más que probables efectos colaterales no deseados, como los daños a equipos de terceras partes inocentes. Todo indica que de manera más o menos soterrada, las ciberescaramuzas entre compañías atacadas y ciberarmas ilegítimas (individuales o apoyadas por Estados hostiles) se estaban produciendo en una escalada preocupante.

*"cuando se actúa en hacking back se pone a inocentes en riesgo"*

*"Estamos en una especie de Salvaje Oeste en estos momentos"*, llegó a manifestar Michael McCaul, presidente del Comité del Senado para la Seguridad Interior, e igual de preocupante fue Tom Kellermann, antiguo miembro de la Comisión de Ciberseguridad del gobierno Obama, al reconocer que había casos de *"defensa activa"*, si bien matizó que no era una corriente generalizada sino que se producían de forma *"muy selectiva"*. Terminó diciendo que *"cuando se actúa en hacking back se pone a inocentes en riesgo"*. El ya citado Ciber-Zar manifestó que había que *"ser realmente cauteloso a la hora de llevar a cabo actividades que sean hacking back o incluso las que algunos intentan llamar <<defensa activa>>".*

## ¿Tiene encaje normativo el hacking back?

Haremos aquí solo una aproximación genérica a la normativa vigente en España y en Estados Unidos, sin dejar de recordar que hablamos de actividades de ámbito privado exclusivamente, por más que las personas cuyas declaraciones hemos mencionado hayan tenido carácter público en algún momento y, sobre todo, insistiendo en que las actividades de *hacking back* no suponen una potencial preocupación de futuro sino un riesgo actual y grave, si tenemos en cuenta que las leyes de nuestro entorno no amparan la ciber-retorsión.

En España, el acceso no autorizado a equipos informáticos ajenos supone un delito del artículo 197 del Código Penal. Su artículo 264, por otro lado, recoge el delito de daños informáticos, describiendo como punible la actuación de quien, sin autorización y de manera grave, entre otras cosas borrase o dañase datos, programas informáticos o documentos electrónicos. Es también delito obstaculizar de manera grave el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo o haciendo inaccesibles datos informáticos. Y habrá que convenir en que toda actividad de ciber-retorsión implica, necesariamente, el acceso a equipos informáticos ajenos y, en ocasiones, la causación de daños a los mismos.

En Estados Unidos, una de las normas de ciberseguridad por excelencia es la *Computer Fraud and Abuse Act* (CFAA), 18 U.S.C. 1030, una ley ya antigua pero que ha sufrido numerosas *actualizaciones* a rebufo del desarrollo tecnológico. Esta norma también prevé como delictivas las actividades de acceso no autorizado a sistemas informáticos ajenos. Inicialmente la norma había de prevenir los ataques a sistemas públicos o protegidos, pero con el tiempo se produjo una extensión de su ámbito de aplicación sobre la base de ampliar el concepto de equipo protegido hasta prácticamente incluir todo aquél desde el cual se pudieran ejecutar actividades de comercio electrónico.

Estando razonablemente clara la ilicitud de la autodefensa del ciberatacado extramuros de los mecanismos de denuncia ante la fiscalía o los cuerpos y fuerzas de seguridad del Estado, no está de más plantear si existen supuestos que supongan una excepción a la norma prohibitiva.

En caso norteamericano (como en el español) la norma no permite el *hacking back* ni siquiera para recuperar los datos que el ciberdelincuente haya podido sustraer. Se parte de que, como en la mayoría de los casos los ciberatacantes utilizan equipos de terceros inocentes como plataforma para sus ataques, el mero intento del perjudicado de recuperar lo sustraído es susceptible de generar un daño en los equipos de dichos inocentes.

En España, el remedio ante la prohibición de acceso para bloqueo del ataque hay que pasa por acudir al concepto de legítima defensa. El artículo 20 del CP la recoge en su apartado 4º como eximente, es decir, generando la imposibilidad del castigo a la persona en quien concurre. En pocas palabras, una acción voluntaria y dañosa realizada por quien se está defendiendo de un ataque ilegítimo no puede ser castigada penalmente, siempre (i) que la agresión de la que se defiende sea ilegítima, (ii) que el medio de defensa empleado sea racionalmente necesario y (iii) que la víctima no haya provocado suficientemente al agresor. Se describe, en resumidas cuentas, una situación en que la actuación ofensiva de contraataque (o *hackback* en este caso) es *lo único que la víctima puede hacer para protegerse.*

*"valoremos la posibilidad de una ciber-retorsión bajo el prisma del derecho español."*

En el mundo cibernético, lo evidente es que los modos de actuación de los ciberdelincuentes no tienen parangón ni réplica (al menos oficialmente admitida) en las estructuras policiales de los estados. Y aquí, dado que las fuerzas y cuerpos de seguridad de los Estados no parecen tener capacidad real de proteger de manera pronta a sus ciudadanos, bien puede entenderse que concurren los requisitos legales reseñados.

Dejando de lado hipotéticas cuestiones de orden estatal, en el sentido de un eventual acto de ciberhostilidad bélica si el asunto de Corea hubiera sido patrocinado por Pyongyang (como sostienen algunos analistas, en contra del criterio de otros igualmente reputados como Brian Krebs o Bruce Scheneier) o directamente perpetrado por ciberarmas coreanas, centremos la cuestión en lo privado y valoremos la posibilidad de una *ciber-retorsión* bajo el prisma del derecho español.

¿Y si el medio español ciberatacado hubiera logrado identificar a su atacante y se las ingeniara para atacar la plataforma desde la que se le agredió, destruyendo la capacidad operativa de la misma? ¿no habría existido aquí una agresión ilegítima de los ciberatacantes contra la víctima?

¿Y no habría sido racionalmente necesario el medio empleado por la víctima en su defensa?¿no podría aplicarse, en suma, a este supuesto la eximente de legítima defensa?

En nuestro derecho los elementos apuntan a que el supuesto sería, cuanto menos, dudoso, y en nuestra opinión, la ley debería decantarse del lado del ofendido. Lo cierto es que mientras la ley no avance lo suficiente y las autoridades puedan garantizar cierto grado de ciberprotección a sus ciudadanos, compañías e instituciones, un sentido racional de la justicia material parece reconocer a las cibervíctimas cierto margen de defensa personal frente a los ciberataques. En esta línea, todo apunta a que la *ciber-retorsión* será un concepto de uso generalizado.

Pero no todo es tan transparente. Nuestro derecho penal recoge el delito de *"ejercicio arbitrario del propio derecho"* (art. 455 del CP), que castiga con multa de seis a doce meses a quien *"para realizar un derecho propio, actuando fuera de las vías legales, empleare violencia, intimidación o fuerza en las cosas"*.

Este peculiar delito supone que el titular de un derecho legítimo sufre un ilegítimo ataque y actúa al margen del cauce legal, auto-protegiéndose de manera activa acudiendo a vías de fuerza.

Está aún por ver qué interpretación hacen los tribunales en relación con la perpetración de un ciberataque como respuesta a otro previo para recuperar lo que de modo remoto se ha robado.. El caso, lejos de ser teórico, cuadra al milímetro con una de las vertientes del *hackback* que parecen repeler menos al espíritu de la norma, en tanto que no persigue una mera la ciber-venganza a través de los daños, sino que busca la recuperación de datos robados por los ciberdelincuentes (el denominado *stolen data retrieval*, un servicio ya ofertado por varias compañías privadas).

La mera idea de que la víctima (sea un banco o un particular) tenga que limitarse a denunciar y a esperar soluciones puede resultar aberrante para cualquier persona involucrada en las TIC desde la parte de la ciberseguridad, atendida la falta de medios técnicos que aqueja a las fuerzas de seguridad en comparación con los medios de los ciberdelincuentes especializados.

A modo de conclusión, los Estados, si no quieren perder una batalla decisiva en el seno de una guerra mucho más amplia, deben afrontar sin demora dos retos muy específicos.

El primero, potenciar de manera urgente las cibercapacidades de las fuerzas y cuerpos de seguridad y de los juzgados y tribunales, posibilitando así el acceso de particulares y empresas a una efectiva y pronta ciberprotección de sus derechos, enervando la previsible tendencia del sector privado a apelar a la auto-ciberdefensa como respuesta al sentimiento de desprotección. Es cierto que la creación de la Fiscalía contra la Criminalidad Informática en España ha supuesto un avance, pero aún resta proveerla de medios técnicos efectivos.

El segundo, legislar prontamente y de manera clara sobre las materias relacionadas con la ciberseguridad de empresas y particulares, partiendo de reconocer la realidad autónoma y extraordinariamente relevante del ciberespacio en las relaciones entre agentes del sector privado.

En definitiva, los Estados han de luchar con todas las armas legislativas a su alcance, dentro del marco del estado de derecho, para evitar que la gráfica referencia al Salvaje Oeste que hizo Michael McCaul se convierta en una realidad generalizada.

# 3 Entrevista a Fco. Javier García Carmona
## Relaciones Externas y Programas Europeos. Dirección de Seguridad Corporativa de Iberdrola.

**1. ¿Cómo estructura un gran operador energético multinacional la protección de activos digitales e infraestructuras críticas? ¿Cuál es el modelo organizativo que lo soporta? ¿Podría explicar brevemente cuál es la función del Departamento de seguridad Corporativo de Iberdrola?**

Una de las principales acciones acometidas ha sido la integración en una misma área organizativa de las actividades de protección de todos los activos de la compañía: bienes, personas e información. Esta integración se produjo en el año 2001; siendo Iberdrola la primera compañía que opto por esta fórmula. De esta forma, cobran sentido y se dota de  contenido a los términos "seguridad integral" y "seguridad corporativa", creando una función habilitadora para el negocio de Iberdrola, reforzando así la aportación del Departamento de Seguridad.

Para ello, Iberdrola ha llevado a cabo un trabajo continuo durante los últimos años con los siguientes objetivos: hacer que la  entienda la necesidad y la aportación de valor de la estructura de protección desarrollada; aumentar el nivel de concienciación general en materia de seguridad, haciéndole entender que la seguridad en su concepción integral es un problema intrínseco a la actividad de la  y de los propios procesos de negocio.

El Departamento de Seguridad Corporativa ha sido alumbrado como un departamento de ingeniería, que si bien no focaliza el desarrollo de su actividad en el propio negocio eléctrico y energético, si lo hace en los riesgos asociados a los bienes, personas e información derivados de dicha actividad, de los cuales son buenos conocedores.

Para ello propone estrategias de defensa de personas, infraestructuras, información y sistemas informáticos, no sólo relacionados con las TIC corporativas sino también de las OT, propias de la actividad industrial. Asimismo se cuentan con mecanismos de colaboración público-privada, que permite intercambiar conocimientos y colaboración con en los agentes reguladores, entes de normalización, protección de infraestructuras críticas, y con las Fuerzas y Cuerpos de Seguridad del Estado.

La cultura de seguridad integral no es nueva en la compañía, ya que se lleva trabajando en ella cerca de 15 años, pero si que es cierto que en el último trienio ha calado de forma mucho más fuerte en el mercado español. La integración y consolidación de todas las actividades y funciones de seguridad en un solo departamento organizativo, es un claro elemento facilitador para todas aquellas s que han sido o serán operadores de infraestructuras críticas, tanto a la hora de cumplir con la normativa homónima así como para implementar de forma efectiva estrategias de protección 360º o integrales.

En Iberdrola, esta integración supone grandes beneficios en términos de eficacia, dado que la misma unidad organizativa es la encargada de proteger desde las infraestructuras de generación y distribución eléctrica hasta los edificios administrativos o la información, ya sea en formato digital o físico. Esta cultura de gestión del cambio organizativa ha permitido que, cada vez que se aborde cualquier tipo de iniciativa que suponga un cambio en un proceso de negocio, el Departamento de Seguridad Corporativa interviene, realizando una función consultiva.

Organizativamente, el Departamento de Seguridad Corporativa está integrado en la Dirección de Recursos y Finanzas, erigido como una subdirección general, lo cual denota el peso jerárquico y la importancia que la otorga a dicha función.

**2. ¿Cuáles son las principales amenazas cibernéticas que enfrenta una empresa de la naturaleza y tamaño de Iberdrola? ¿Cómo afronta Iberdrola los retos asociados a la ciberseguridad industrial?**

Iberdrola, como operador de un servicio universal que es crítico, tanto en la vertiente de generación de energía como en su transporte y distribución, está expuesto y toma en consideración las ciberamenazas así como las amenazas de carácter físico. Así pues, los vectores de amenaza que definen las estrategias de protección de la son aquellas que puedan afectar a la población (no perdamos de vista que la opera infraestructuras nucleares), así como aquellas que supongan una interrupción del negocio. En ambos casos, la aproximación de defensa es similar.

Ante este nuevo escenario de amenazas, extremadamente complejo y donde cada vez más aumenta la exposición a los riesgos de seguridad física, que intersecan con los riesgos cibernéticos, Iberdrola desarrolla un concepto de protección que integra ambos ámbitos.

**3. Según algunas estimaciones, en el año 2020 más de 80% de los contadores eléctricos serán smartmeters. ¿Qué riesgos supone la digitalización e interconexión de diversos sistemas industriales en el sector energético? ¿estamos preparados para afrontar las amenazas contra sistemas ICS/SCADA?**

Efectivamente, en la actualidad, nos encontramos en la etapa de sustitución de los equipos de medida regulada por la *Orden ITC/3860/2007*, de 28 de diciembre. De este modo, todos los contadores analógicos serán sustituidos antes del 31 de diciembre de 2018, de acuerdo a los hitos establecidos en el Plan de Sustitución, por contadores inteligente o smartmeters. Por su parte, los equipos de medida quedarán regulados por el *Real Decreto 1110/2007* y la *Orden ITC/3022/2007*. Este Plan de Sustitución no supone solo el cambio de los contadores de abonados y empresas, sino también la infraestructura de distribución eléctrica así como de los sistemas y procesos de backoffice.

Ante la creciente interconexión derivada de los mecanismos de digitalización de los contadores, las principales amenazas a las que nos enfrentamos son:

- Inexistencia de estándares unificados de seguridad en el mundo del *smartmetering*.
- Los fabricantes tecnológicos actúan en muchas ocasiones como *stoppers*, ya que cada cual quiere imponer su estándar.
- Actualmente los costes de securización y protección del sistema de contadores inteligentes, sin ser una medida obligatoria, los asume la eléctrica.

Iberdrola, al igual que el resto de las eléctricas españolas, es muy sensible a estos riesgos

y derivado de ello, emplea y dedica todos los recursos a su alcance para disponer en el entorno de los smartmeters toda una plataforma de seguridad que garantice el servicio y máxima fiabilidad de dicha solución.

**4. ¿Cree que sería necesario el desarrollo de políticas incentivadoras estatales para fomentar la adopción por parte de la industria de mecanismos de ciberseguridad?**

El Estado debería adoptar unas políticas proactivas y positivas, con menos medidas impositivas. Además, debería fomentar una política inclusiva para con la industria a fin de evitar la unilateralidad a la hora de lanzar procesos legislativos y normativos, desarrollando marcos de políticas incentivadoras.

Dichas políticas deberían fomentar la distribución de los costes de la ciberseguridad y la protección sobre todos los actores involucrados, premiando a las organizaciones comprometidas con la protección de sus activos.

Entre los esfuerzos normativos desarrollados, cabe destacar el lanzamiento de un estándar común de seguridad dirigido principalmente a los Operadores Críticos relativo a la seguridad en el proceso de generación, distribución y almacenamiento de energía eléctrica, que será presentado a corto plazo.

**5. ¿Considera que la industria española de ciberseguridad, tanto de soluciones tecnológicas como de servicios, tiene una madurez adecuada para satisfacer la creciente demanda del mercado nacional?**

Si, actualmente España ocupa el tercer puesto cuanto a capacidades, conocimientos y experiencia en ciberseguridad y ciberdefensa. Fruto de ello, es la fuga de capital intelectual español en la materia hacia empresas americanas e israelitas y, con menor incidencia, en el resto de Europa. España se está convirtiendo en un ecosistema de alto nivel en la generación de profesionales de ciberseguridad, si bien la situación actual hace que muchos de ellos opten por trabajar para empresas extranjeras, ya sea dentro o, como sucede con mayor asiduidad, fuera del territorio nacional. España está actuando como un centro de offshoring en ciberseguridad.

Se deberían desarrollar políticas públicas que reforzase el I+D+i en el ámbito de la ciberseguridad, impulsado la creación de startups pioneras en el desarrollo de soluciones y productos de ciberprotección.

**6. ¿El Estado tiene la capacidad de defender los intereses en el ciberespacio de las grandes corporaciones como Iberdrola? ¿Dispone de mecanismos adecuados, efectivos y ágiles? ¿Cree que las empresas deberían tener cierta potestad para responder de forma unilateral ante determinados incidentes de seguridad?**

En cierta medida si, la industria suele desarrollar medidas de protección reactivas, mientras que el Estado fomenta las estrategia prospectivas y de inteligencia. Sin embargo la industria, al igual que cualquier empresa, parte de una situación de cierta desventaja frente a los atacantes. En este sentido, al Estado le sucede lo mismo: se encuentra con grandes barreras legislativas y jurídicas, sobre todo a nivel internacional, pero no adolece de capacidades.

**7. Actualmente se habla de forma recurrente de ciberinteligencia. ¿Cree que este tipo de aproximaciones son necesarios en la gran empresa española?**

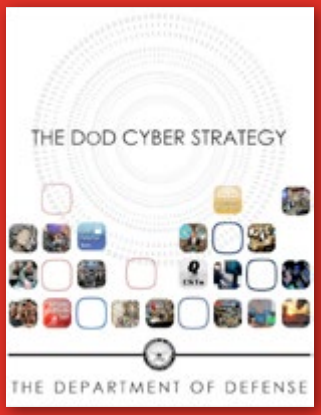
Son imprescindibles. Las grandes s deberían tener una unidad funcional de inteligencia que, entre otras, explotase y generase valor con la inteligencia de seguridad, de amenazas, ya que la propia madurez de una empresa como Iberdrola y su infraestructura hace que cada vez genere más volumetría de información de seguridad que debe ser explotada, para desarrollar no sólo una aproximación correctiva y preventiva, sino también prospectiva.

Toda esa información, junto con la que provienen del exterior de la Organización, como fuentes abiertas y públicas, tienen un valor inmenso, pero no sabemos explotarlas adecuadamente, ya que no se disponen de recursos para explotarlos y usarlos. Es una cuestión de tiempo y de recursos.

Además, el desarrollo de estas capacidades habilitarían el intercambio de información entre agentes del sector y la colaboración público privada en el sector industrial.

# 4 Informes y análisis sobre ciberseguridad publicados en abril de 2015

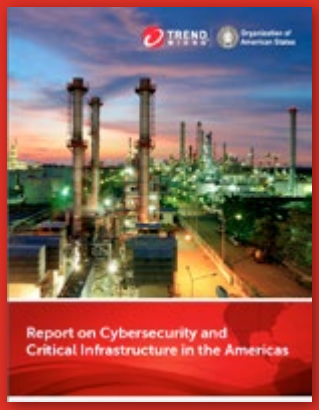
The DoD Cyber Strategy (U.S Department of Defense)




Cloud Security Guide for SME (ENISA)

APT30 and the mechanics (Fireye)

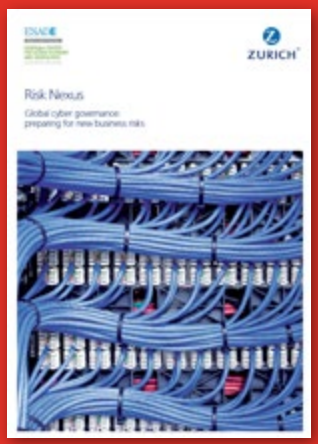
Report on Cybersecurity and Critical Infraestructure in the Americas (OAS y Trend Micro)



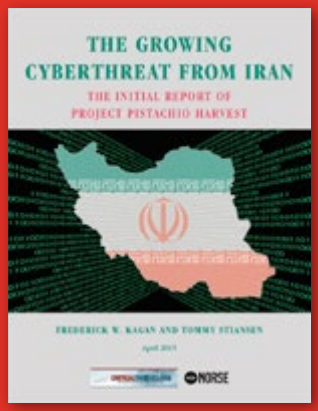

VOLATILE CEDAR (CheckPoint)

Informe Anual de Seguridad Nacional 2014 (Presidencia de Gobierno)

Global cyber governance: preparing for new business risks (ESADE y ZURICH)




The growing cyberthreat from Iran (NORSE)



# 5 Herramientas del analista: Collective Intelligence Framework (CIF)

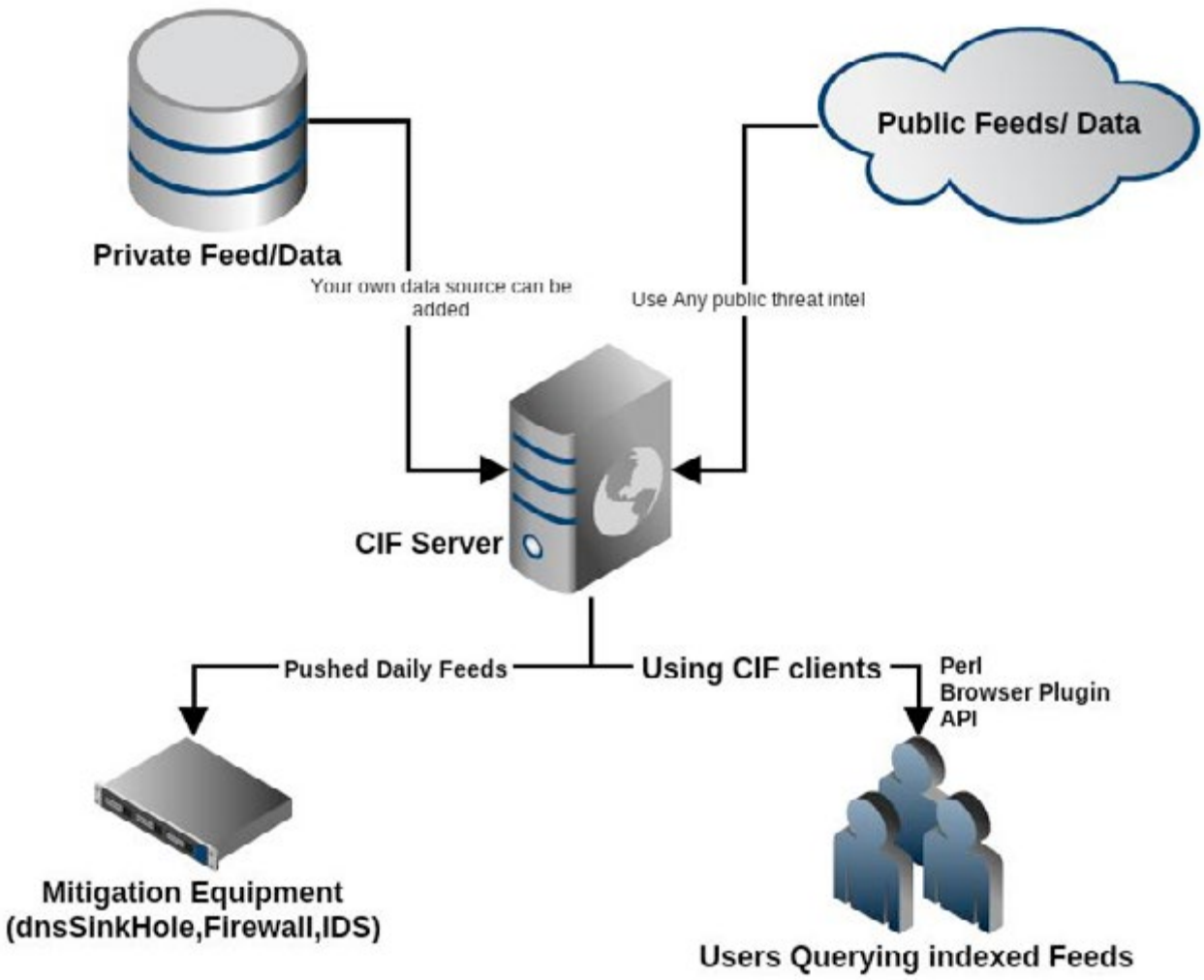



Ilustración 1: Arquitectura del Framework de Inteligencia Colectiva (CIF).

El uso efectivo de la inteligencia de ciberamenazas es una herramienta importante y efectiva para defenderse frente actividades maliciosas en internet.

El *Framework de Inteligencia Colectiva* (Collective Intelligence Framework –CIF-) es una infraestructura cliente/servidor opensource gratuita que permite el intercambio de datos de inteligencia de ciberamenazas así como combinar los datos provenientes de múltiples fuentes. El proyecto CIF vio la luz en 2009, siendo desarrollado por la *Research and Education Network Information Sharing and Analysis Center* (REN-ISAC).

La solución, cuyo core está desarrollado en Perl, incluye un servidor que recolecta y almacena la información relativa a las ciberamenazas, tales como direcciones IP con actividad maliciosa, números ASN, direcciones de email, dominios o URLs junto con otros atributos de especial interés para los analistas: severidad de la amenaza, tipología y confianza (reputación) en la fuente de datos. Estos datos pueden ser accedidos a través de diversos clientes. El cliente estándar incluido en la plataforma es una utilidad de línea de comandos desarrollado también en Perl, si bien existen plugins para navegadores web estándar.

Asimismo, la solución permite un control de acceso granular a la información, almacenada en formato *IODEF*, si bien puede exportar la información en diversos formatos, generando "inteligencia accionable" que le permite interactuar con sistemas de detección y prevención de intrusiones (IDS/IPS), como pueden ser reglas para *Snort* o para firewalls basados en *iptables*.

En definitiva, CIF ayuda a analizar, normalizar, almacenar, procesar correos, consultar y producir conjuntos de datos de inteligencia de amenazas de una forma eficaz.

Ilustración 2: Proceso de generación de ciberinteligencia con CIF.

# 6 Análisis de los ciberataques del mes de abril de 2015

**AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.**
**Cybersecurity advisor, Eleven Paths (Telefónica).**

Este primer mes de la primavera de 2015 ha mostrado un crecimiento sostenido en ciberataques a nivel global.

## CIBERCRIMEN

En cuanto a las actividades criminales, si cerrábamos el mes anterior destacando el ataque a Lufthansa, de nuevo una aerolínea tiene un triste papel protagónico ante un caso de fraude bancario online. La aerolínea irlandesa de bajo coste *Ryanair confirmó que unos 4,5 M € fueron sido extraídos fraudulentamente* de una de sus cuentas bancarias a través de una operación efectuada desde un banco chino.

A comienzos de mes, el equipo de analistas de Eset publicó un análisis detallado de la *operación Buhtrap*, guardando ciertas similitudes técnicas con *Carbanak* y *Anunak* y materializada a través de una nueva cepa de malware que recopila información de equipos informáticos rusos, focalizados en los departamentos de contabilidad de diversas empresas privadas moscovitas.

СЧЕТ № 21 от 20.03.2014 г.

Исполнитель: ООО НПП "Стройинжиниринг"
Адрес: 629300, ЯНАО, г. Новый Уренгой, ул.Глухариная, 2/4, левое крыло
Тел/факс: (3494) 24-44-01; 24-44-02
Банковские реквизиты:

| | | | |
|---|---|---|---|
| Получатель: | ООО НПП "Стройинжиниринг" | Р/сч | 40702810600000001323 |
| ИНН/КПП: | 8904043570/890401001 | | |
| Банк получателя: | ф-л ПФБ (ОАО) в г.Новый Уренгой,Тюменская обл. г.Новый Уренгой | БИК | 047195753 |
| | | К/сч | 30101810700000000753 |

Заказчик: Общество с ограниченной ответственностью "Теле МИГ"
Адрес: 629300, ЯНАО, г. Новый Уренгой, ул. Таежная, д.78
Телефон: 22-22-22, 22-22-27, 22-22-25

Валюта: RUB

| № | Наименование товара | Единица измерения | Количество | Цена | Сумма |
|---|---|---|---|---|---|
| 1 | Оказание услуг по организации повышения квалификации ИТР по договору №18 от 13.03.2014 г. по теме: "Электроснабжение" | чел. | 3 | 12 000,00 | 36 000,00 |
| | | | | ИТОГО: | 36 000,00 |
| | | | | НДС не предусмотрен (п.2 ст.346.11 гл.26.2 НК РФ) | - |
| | | | | Всего к оплате | 36 000,00 |

Заместитель директора О.Н. Буксирнова

Ilustración 1: Documentos Word conteniendo el payload malicioso explotado en la operación Buhtrap.

Por otra parte, hemos asistido a uno de los primeros casos de ciberataques recíprocos entre grupos de cibercriminales, protagonizados por los grupos *Hellsing y Naikon*, con sendas campañas de ataques dirigidos, el segundo como una respuesta o hack-back ante una campaña del primero. Estas "ciberescaramuzas" son cada vez más habituales entre agrupaciones criminales rivales.

## CIBERESPIONAJE

El mes de abril ha sido especialmente activo en cuanto a campañas de ciberespionaje.

A mediados de mes, se hacía público el descubrimiento de *APT30, un campaña detectada y reportada por FireEye*, mostrando como un grupo, con supuesto apoyo estatal, ha estado accediendo a información clave de entidades gubernamentales (con especial énfasis en agencias de inteligencia) y grandes corporaciones en el sudeste asiático e India durante la última década a través de sofisticados vectores de ataque dirigidos.

Ilustración 2: Mapa de países afectados por APT30 confirmados y potenciales.

Por otra parte, de acuerdo con un grupo de analistas de *Blue Coat, un grupo de hackers de origen árabe* fueron capaces de infiltrarse en las redes de las Fuerzas de Defensa Israelíes (IDF) a través de una campaña de spearphising cuyos emails rezaban "Girls of the Israel Defense Forces". Dichos emails adjuntaban familias de troyanos conocidos, como Poison Ivy.

Finalmente, el equipo de investigación e inteligencia de amenazas de Check Point publicó un interesante análisis de la que han denominado *Operación Volatile Cedar*, operativa desde finales de 2012, siendo una campaña cuidadosamente orquestada y focalizada en personas, empresas e instituciones de todo el mundo.

Esta campaña, liderada por un grupo especializado en APTs de origen libanés y con potencial apoyo estatal o político por la verticalización de sus objetivos (descartando motivación económica en los ataques), ha conseguido penetrar con éxito en un gran número de objetivos utilizando diversas técnicas de ataque y, en concreto, a través un implante malware a medida cuyo nombre en código es Explosive.

## HACKTIVISMO

Sin embargo, han sido las notables campañas hacktivistas las que han copado los titulares a lo largo del mes. Tras los ataques de un grupo activista pro-Daesh a la cadena francesa TV5, el grupo de comunicación belga Rossel se ha convertido en la segunda organización de habla francesa en ser víctima de un ciberataque dirigido en pocos días. *Durante varias horas, la edición digital de "Le Soir"*, periódico del grupo, sufrió un ataque de denegación de servicio. Un grupo que se autoproclama a favor del IS reclamó la autoría del ataque.

Al mismo tiempo, un grupo de ciberyihadistas de origen tunecino autodenominado “Fallaga Team” *atacaba diversas webs del gobierno de la región de Wallon*. Esta creciente escalada sobre objetivos belgas parece responder a la participación activa del gobierno bruselense en la campaña liderada por EEUU contra el Daesh en Siria e Irak.

El 7 de abril también es una fecha importante para los hacktivistas de todo el mundo. El mismo día, durante los últimos cuatro años, diversos grupos hacktivistas focalizan sus ataques sobre un solo objetivo: Israel, *desarrollando la denominada #OpIsrael*, como protesta a las acciones ofensivas sobre el pueblo palestino. Las capacidades defensivas del Shin Bet, la Agencia de Seguridad de Israel y el Centro Nacional de Ciberdefensa, permitieron reducir el impacto de dicha campaña, cuyos daños fueron marginales, siendo sus impactos más significativos:

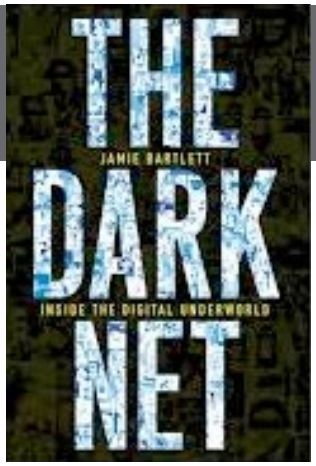
- Denegación de servicio sobre la web del Israeli Center for Educational Excellence
- Vulneración de más de 150.000 número de teléfono y cuentas de Facebook, Gmail y Hotmail de usuarios israelíes
- Defacement de la web oficial del cantante israelí Shalom Hanoch, cuyo contenido fue sustituido por imágenes de los lugares sagrados musulmanes en Jerusalem acompañado por un mensaje de AnonGhost

# 7 Recomendaciones

## 7.1 Libros y películas

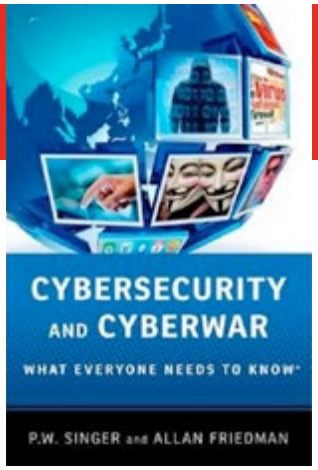
**Película:**
**JUEGOS DE GUERRA (WAR GAMES, 1983)**

Sinopsis: David es un joven conocedor de todo lo referente a la seguridad informática: capaz de saltarse los más avanzados sistemas de seguridad, consigue acceso a diversos códigos secretos gubernamentales y entiende la informática como un juego, un reto. Pero el juego se complica cuando inconscientemente conecta su PC al del Departamento de Defensa (DoD) norteamericano, encargado de la gestión del sistema de defensa nuclear, desencadenando una situación de peligro de proporciones incontrolables. Ayudado por su novia y por un "genio" de los ordenadores tendrá que evitar, en una lucha contrarreloj, el mayor conflicto mundial de todos los tiempos: la Tercera Guerra Mundial. Esta película es uno de los clásicos imprescindibles para introducirse en la seguridad de la información.




**Libro:**
**THE DARK NET**

**Autor:** Jamie Bartlett
**Num. Paginas:** 320
**Editorial:** Windmill Books
**Año:** 2015
**Precio:** 10.00 Euros
**Sinopsis:** Este libro nos ilustra sobre el funcionamiento del lado mas oscuro de internet.

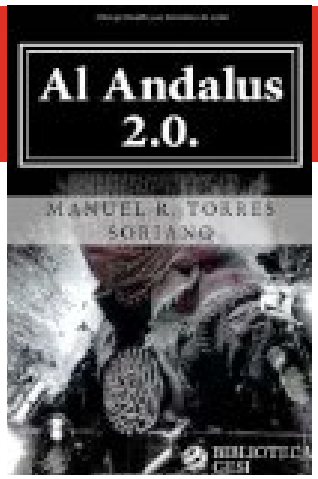



## Libro:
## CYBERSECURITY AND CYBERWAR

**Autor:** P.W.SINGER y Allan Friedman
**Num. Paginas:** 320
**Editorial:** OUP USA
**Año:** 2014
**Precio:** 13.50 Euros
**Sinopsis:** Este libro expone todos los conceptos necesarios para que cualquier ciudadano pueda comprender la importancia estratégica que tiene el ciberespacio para el desarrollo socio-económico de las naciones.

## Libro:
## CYBERWAR WILL NOT TAKE PLACE

**Autor:** Thomas Rid
**Num. Paginas:** 256
**Editorial:** C Hurst & Co Publishers Ltd
**Año:** 2013
**Precio:** 17.50 Euros
**Sinopsis:** El autor desmitifica el alarmismo de una inminente ciberguerra. Haciendo uso de los principales ciberataques acontecidos hasta el momento, argumenta que no estamos inmersos, ni estaremos en el medio plazo, en una guerra cibernética.




## Libro:
## AL ANDALUS 2.0

**Autor:** Manuel R. Torres Soriano
**Num. Paginas:** 266
**Editorial:** Biblioteca Gesi
**Año:** 2014
**Precio:** 14.00 Euros
**Sinopsis:** Esta obra analiza la explosiva combinación entre terrorismo, nuevas tecnologías de la información y agravios históricos.

# 7.2 Webs recomendadas

**https://www.schneier.com/**
Blog personal de Bruce Schneier, uno de los principales gurús del campo de la seguridad de la Información.

**http://slashdot.org/**
Sitio web de noticias donde se fomenta el debate y dialogo entre los usuarios.

**https://threatpost.com/**
Sitio de noticias de Kasperky Lab.

**http://www.flu-project.com/**
Blog que tiene como objetivo enseñar y concienciar a los usuarios sobre los problemas producidos por el malware.

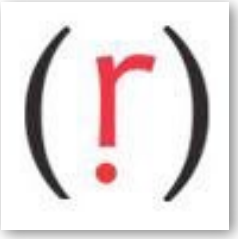
**http://cnec.icfs.es/**
Sitio web del Centro Nacional de Excelencia en Ciberseguridad.

**http://www.enisa.europa.eu/**
Sitio web de la Agencia Europea para la seguridad de la información y las redes.

# 7.3 Cuentas de Twitter

**@EC3Europol**

**@securityartwork**



**@INTERPOL_Cyber**

**@ElevenPaths**

**@CIGTR**

# 8 Eventos

| FECHA | LUGAR | ORGANIZADOR | TÍTULO | URL |
|---|---|---|---|---|
| 5-8 mayo | Beijing, China | Beihang University | 11st Information Security Practice and Experience Conference (ISPEC) 2015 | http://icsd.i2r.a-star.edu.sg/ispec2015/ |
| 7-may | Washington | Checkpoint | Check Point Experience Conference USA | http://www.checkpoint.com/cpx-2015/index.html |
| 13-may | Bilbao | Centro de Ciberseguridad Industrial | Soluciones para proteger los sistemas de automatización industrial | https://www.cci-es.org/web/cci/detalle-evento/-/journal_content/56/10694/142405 |
| 20-may | Madrid | ISMS Forum | XVII ISMS Forum Spain | https://www.ismsforum.es/noticias/noticia.php?idnoticia=610 |
| 21-may | Bilbao | Nextel | NextSecure | https://nextsecure.es/?utm_source=seguritecniaweb&utm_medium=mediocomunicacion&utm_campaign=nextsecure2015#inscripcion |
| 22-23 mayo | Madrid | Varios | Jornadas X1RedMasSegura 2015 | http://www.x1redmassegura.com/ |
| 27-28 mayo | Barcelona | Security Forum | Security Forum 2015 | http://www.securityforum.es/presentacion-security-forum/ |
| 2-4 junio | Londres | InfoSecurity Europe | InfoSecurity Europe 2015 | http://www.infosecurityeurope.com/ |
| 2-3 junio | Buenos Aires | Centro de Ciberseguridad Industrial | IV Congreso Internacional de Ciberseguridad Industrial | https://www.cci-es.org/web/cci/detalle-congreso/-/journal_content/56/10694/135953 |

www.realinstitutoelcano.org
www.blog.rielcano.org
www.globalpresence.realinstitutoelcano.org

www.thiber.org
twitter.com/thiber_esp
linkedin.com/groups/THIBER-the-cybersecurity-think-tank