ABRIL 2015 / Nº 2

CIBER elcano

Desarrollado por:

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 Opinión ciberelcano 15

4 Entrevista a GD. Carlos Gómez López de Medina 21

5 Informes y análisis sobre ciberseguridad publicados en marzo 2015 25

6 Herramientas del analista 26

7 Análisis de los ciberataques del mes de marzo de 2015 28

8 Recomendaciones

8.1 Libros y películas 30

8.2 Webs recomendadas 32

8.3 Cuentas de Twitter 32

9 Eventos 33

1 COMENTARIO CIBERELCANO:

En favor de una política nacional de ciberseguridad en España

AUTORES:
Félix Arteaga. Investigador principal de Seguridad y Defensa. Real Instituto Elcano.
Enrique Fojón Chamorro. Subdirector de THIBER, the cybersecurity Think Tank.

El Real Instituto Elcano, en colaboración con *Thiber*, acaba de lanzar un informe de situación mensual: *Ciber elcano.* No es la única fuente de información en español, ya que existen medios impresos como las revistas Red Seguridad y SIC y sitios web como el del Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Criptológico Nacional (CCN-CNI) donde se divulgan ampliamente las cuestiones de ciberseguridad. Pero su peculiaridad reside en que da prioridad a las cuestiones relacionadas con la gobernanza, gestión y política de la ciberseguridad. Trata, por tanto, de **fomentar la cultura de ciberseguridad** entre los decisores en los distintos nivelesestatales, subestatales, empresariales, industriales, tecnológicos y universitarios, públicos y privados, implicados en la gestión de la ciberseguridad.

A diferencia de otras funciones públicas como la diplomacia, la seguridad y la defensa, la ciberseguridad carece de un marco de conocimiento preexistente y se construye –en España y fuera de ella– desde cero y mediante procesos de experimentación, acierto y error, y copia de las mejores prácticas conocidas. En las estanterías del conocimiento y en las academias de funcionarios no existen todavía materiales que faciliten el despegue y consolidación de esta nueva función estatal, vital para la seguridad y prosperidad de los españoles, como han reconocido las Estrategias de Seguridad Nacional.

La primera de ellas *incluyó en 2011* las ciberamenazas y los ciberataques entre los riesgos principales para la seguridad nacional, al igual que *la vigente aprobada en 2013*. Desde entonces se ha trabajado deprisa para hacer hueco a la recién llegada entre las funciones tradicionales de gobierno. A la búsqueda de la gobernanza, se dispone ya de una primera visión –estrategia– de lo que debe ser la ciberseguridad y de una organización básica –sistema– encarga de desarrollar aquella visión. Del mismo modo, desde el punto de vista operativo nuestro país dispone de varios Centros de Respuesta ante Incidencias Informáticas (CERT) nacionales y autonómicos, un Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, una Dirección General de Tecnologías de la Información y Comunicación de la Administración General del Estado y una Oficina de Coordinación Cibernética en el Centro Nacional de Protección de Infraestructuras Críticas. Además, el gobierno parece haber identificado la **necesidad de disponer de un sector e industria de ciberseguridad de primer nivel**, tal y como refleja en el Plan de Confianza en el ámbito Digital. La gobernanza tiende a consolidarse tras decidir el Gobierno, a principios de 2015, acabar con el sistema de rotación que afectaba a la dirección de la ciberseguridad y residenciar la presidencia del Consejo de Ciberseguridad en el Centro Nacional de Inteligencia (CNI).

"Además de una identidad diferenciada, toda Administración nueva necesita también recursos propios."

Finalizado el aterrizaje, la ciberseguridad debe pasar de su fase de gobernanza actual y dirigirse en el corto plazo hacia la **construcción de una Política Nacional de Ciberseguridad.** Construir una política supone dotar a la ciberseguridad de la misma estructura (dirección, sistema, control y comunicación), instrumentos (tecnológicos, humanos, presupuestarios y normativos), procesos (diseño, ejecución, evaluación y revisión de planes y estrategias) y funciones que cualquier otra política pública, peculiaridades aparte. Se considera que, aun disponiendo la ciberseguridad de algunos elementos propios de una política, todavía carece de otros que la permitan mostrarse como una función estatal diferenciada. Por mencionar algunos de mayor notoriedad, la ciberseguridad no dispondrá de un espacio propio mientras comparta liderazgo y recursos con terceros. La dirección única actual bajo el CNI ofrece mejores oportunidades de gobernanza y desarrollo a la ciberseguridad que la rotación anterior por los diferentes ministerios y agencias. Pero si la ciberseguridad crece en la medida que se espera, deberá alejarse en el futuro de la incubadora de inteligencia donde se encuentra para encontrar su propia autonomía entre las distintas culturas de seguridad vigentes. Además de una identidad diferenciada, toda Administración nueva necesita también recursos propios. La ciberseguridad no puede construirse a coste cero ni contra los recursos limitados de otros ministerios y agencias públicas. Más allá de las declaraciones de intención, los recursos asignados serán los que midan el nivel de ambición y coherencia de cada Gobierno. Y los recursos presupuestarios serán el menor de los problemas a los que se va a enfrentar la ciberseguridad, ya que otros recursos como los de personal capacitado o los tecnológicos van a ser mucho más complicados –y tampoco baratos– de encontrar.

También creemos que lo verdaderamente nacional debe ser la política y no tanto la ciberseguridad. Abogar por una Política Nacional de Ciberseguridad en lugar de una política de ciberseguridad nacional no es un capricho semántico porque el calificativo de nacional añade a la política la inclusión de todos los elementos de la nación –y no sólo de los gubernamentales– a la gestión de la ciberseguridad. **La gobernanza actual debe abrirse a una política nacional que integre más actores y capacidades públicas y privadas.** Hasta ahora se cuenta con el Foro Nacional de Confianza Digital para estudiar y proponer medidas de estímulo en favor de las Tecnologías de la Información y las Comunicaciones, incluidas la de ciberseguridad, pero debe ampliarse y profundizarse tanto a los ámbitos industriales, tecnológicos y educativos implicados en la ciberseguridad como a los sociales y políticos que deben participar en la supervisión y control de una política "nacional" de ciberseguridad.

Finalmente, nos parece que las funciones de la nueva política sujetas a la gobernanza actual –seguridad de la información, gestión de crisis, análisis de riesgos, defensa y explotación y la resiliencia– son adecuadas para afrontar la ciberseguridad desde la perspectiva de los riesgos. Pero la futura política deberá atender también a las oportunidades que abre la ciberseguridad a un mercado donde el volumen de negocio crece a ritmo de dos dígitos en los últimos años (se calcula que el mercado mundial va a pasar de los 68.000 millones de dólares en 2013 a los 120.000 millones en 2020, una fecha en la que estarán interconectados 6.000 millones de usuarios y 25.000 millones de máquinas). Más allá de los peligros, el ciberespacio ofrece oportunidades para crear un tejido industrial innovador, empleos de calidad y capacitación tecnológica. Una visión más amplia debería desarrollar instrumentos de demanda pública, definir prioridades en I+D+i, incentivar las inversiones y crear centros de excelencia, entre otros, para que en España se pase de consumir a producir ciberseguridad.

En definitiva, si la ciberseguridad es tan importante como se dice y si tiene el recorrido y trascendencia que se espera, **es necesario progresar desde el modelo de gobernanza actual**, entre la contingencia y la consolidación, **a uno de política pública de mayor recorrido y más largo plazo.** Desde el Real Instituto Elcano y desde THIBER pretendemos ayudar a la transición con este nuevo producto compartido ***Ciber elcano*** y animamos a quienes nos quieran acompañar en esta nueva tarea a *suscribirse* para recibirlo y a contribuir a su desarrollo.

2 ANALISIS DE ACTUALIDAD INTERNACIONAL:
Sin coordinación efectiva no hay Ciberdefensa

AUTORES:
Dr. José Ramón Coz Fernández. Analista Internacional THIBER. Security Manager y Auditor en PMIC-OTAN
Vicente José Pastor Perez. Jefe de Servicio de Seguridad Empresarial en NCIRC-OTAN

El Centro de Respuesta a Incidentes de la OTAN durante la ejecución del ejercicio Cyber Coalition 2014
Fuente: NATO Communications and Information Agency

INTRODUCCIÓN

Por derecho propio, el ciberespacio se ha convertido en el quinto dominio de las operaciones militares tras la tierra, los mares, el aire y el espacio. Aunque a diferencia del resto de los entornos donde se combate, éste tiene una dimensión física y virtual; por lo que cualquier suceso que ocurra en el ciberespacio tiene efectos en el mundo físico y viceversa. De hecho, la creciente preocupación acerca de la facilidad para realizar acciones casi-anónimas en el ciberespacio que repercutan en el mundo físico ha hecho que este asunto adquiera una relevancia suficiente para atraer el interés de todos respecto a la seguridad cibernética y su influencia sobre la seguridad en otros entornos .

Para defenderse en un medio en el que los adversarios se mueven de manera casi invisible y atacan con impunidad, es esencial la coordinación entre los diferentes guardianes del ciberespacio. No basta conocer lo que se está defendiendo, ni las tácticas, técnicas o procedimientos utilizados por los atacantes. Es necesario disponer de información de alerta temprana. Es vital contar con inteligencia que nos indique cuáles son los cursos de acción más probables antes de que el adversario los lleve a cabo. En este sentido, además de los programas de compartición de información entre los servicios de inteligencia, es necesario extender la colaboración a todos los actores que participan en la ciberdefensa. Es fundamental entregar información a tiempo a las entidades que pueden tomar acciones sobre la misma.

Este artículo pretende mostrar las organizaciones e iniciativas de coordinación que existen en otros países para facilitar la compartición de la información y contribuir a la defensa colectiva del ciberespacio en materia de prevención y respuesta a incidentes de seguridad.

LA CIBERDEFENSA COLECTIVA MÁS AVANZADA

Desde hace varios años, los países avanzados están realizando fuertes inversiones en materia de ciberseguridad. Hoy en día, cualquier capacidad defensiva está basada en las tecnologías de la información y comunicaciones. Sin este soporte, ninguna de las principales infraestructuras de cualquier país no puede funcionar. Además, los riesgos a los que se ven sometidas estas infraestructuras son cada vez mayores y los ataques más sofisticados. Y es que detrás de ellos hay grandes inversiones y apoyo político, lo que complica sobremanera la protección de las mismas.

Ante este nivel de riesgo, es evidente que los gobiernos deben poner en marcha mecanismos que garanticen la seguridad a los ciudadanos. Esta alarma ya ha sido activada en muchos países de nuestro entorno. Por ello, actores como Francia, Reino Unido, Israel, Arabia Saudí, Rusia, India, China o la propia OTAN, están destinando ingentes recursos para poner en marcha varias líneas de inversión relacionadas con el campo de la ciberdefensa. La financiación adicional se destina a nuevas estructuras organizativas, a programas de ingeniera de la información, a la implantación de nuevos procesos, a la formación avanzada o a la investigación.

La complejidad es tal que incluso los países más avanzados no afrontan este gran cambio sin contar con fuertes alianzas. Hace varias décadas, en Estados Unidos ya eran conscientes de que sólo con el apoyo y la coordinación entre diferentes entidades se podía llevar a cabo programas complejos relacionados con la ciberseguridad. Para ello, en virtud de la Directiva Presidencial 63 – que reconocía el potencial devastador de los ataques cibernéticos sobre las infraestructuras físicas del país – se crearon los Centros de Compartición de la Información (ISAC) en sectores como la alimentación, el transporte, el sector financiero o la energía. Estos centros, establecidos desde 1998, ya se encuentran totalmente consolidados.

En el país también existen otras figuras más avanzadas como las Organizaciones de Análisis y Compartición de Información (ISAO) que, dirigidas por la Casa Blanca, permiten a las empresas estadounidenses compartir datos de ciberamenazas entre ellas y el Departamento de Seguridad Interior; el Centro Nacional de Integración de Comunicaciones y Ciberseguridad (NCCIC) o el Centro de Integración de Inteligencia de Ciberamenazas (CTIIC), un centro de fusión de información entre las agencias gubernamentales y el sector privado que posibilita la utilización de inteligencia sobre ciberamenazas en tiempo real como prevención contra ciberataques. Países como Japón, India o Reino Unido también han implantado organizaciones con similares características.

De manera similar, la OTAN también está trabajando para fortalecer esta ciberdefensa colectiva a través de diversas iniciativas. Dentro del marco de la Defensa Inteligente (Smart Defence), existe un conjunto de acciones lideradas por la propia Alianza con el fin de mejorar la cooperación en ciberdefensa mediante la financiación conjunta de proyectos de I+D+i para el desarrollo y adquisición de capacidades relacionadas con la ciberseguridad, con un objetivo de alcanzar un menor coste y una mayor calidad. La idea consiste en que las capacidades desarrolladas bajo estos programas puedan ser utilizadas e integradas posteriormente por los diferentes estados miembros.

Una de ellas es el Proyecto Multinacional para el Desarrollo de Cibercapacidades (MNCD2) que cuenta con la participación de Rumanía, Canadá, Noruega, Holanda o Dinamarca. En la actualidad, MNCD2 comprende tres paquetes de trabajo: el Sistema de Coordinación sobre Ciberincidentes y Ciberinformación (CIICS), la Conciencia Situacional para Ciberdefensa (CDSA) y la Infraestructura Distribuida de Recolección y Correlación Multisensor (DMCCI). Adicionalmente, se está debatiendo la creación de un concepto que permita guiar el establecimiento de equipos de apoyo multinacionales para realizar evaluaciones de seguridad.

Otros proyectos dignos de mencionar son: la Plataforma para la Compartición de Información sobre Malware (MISP), el Programa de Protección de Infraestructuras de la OTAN (NCIRC FOC), los proyectos de coordinación de ejercicios de ciberdefensa y otras iniciativas en investigación y adquisición de cibercapacidades, sobre los que los miembros podrán aprender de experiencias pasadas y tomarlas como referencia para el desarrollo de sus capacidades y/o integrarlas con las propias de la OTAN.

Visita del Consejo Atlántico al Centro de Respuesta a Incidentes de Seguridad Informática de la OTAN en Enero de 2015
Fuente: Biblioteca multimedia de la OTAN

Los ejercicios y simulaciones en el campo de la ciberdefensa son esenciales. La OTAN celebra anualmente, en el mes de noviembre, su ejercicio Cyber Coalition para poner en práctica, detectar problemas y mejorar sus procesos y procedimientos en el área. Este ejercicio va creciendo en número de países participantes año tras año, y su complejidad y sofisticación siguen una evolución similar.

El control del ejercicio Cyber Coalition 2012 se llevó a cabo en el bunker del Cuartel General Supremo de las Fuerzas Aliadas en Europa
Fuente: OTAN

Adicionalmente, existe el Locked Shields, un ejercicio de carácter más técnico que organiza cada año el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN en Tallin (Estonia). Además de la OTAN, en este ejercicio participan varios países aportando miembros al equipo rojo (ataque) o formando su propio equipo azul (defensa).

LA COORDINACIÓN Y COLABORACIÓN EN CIBERDEFENSA

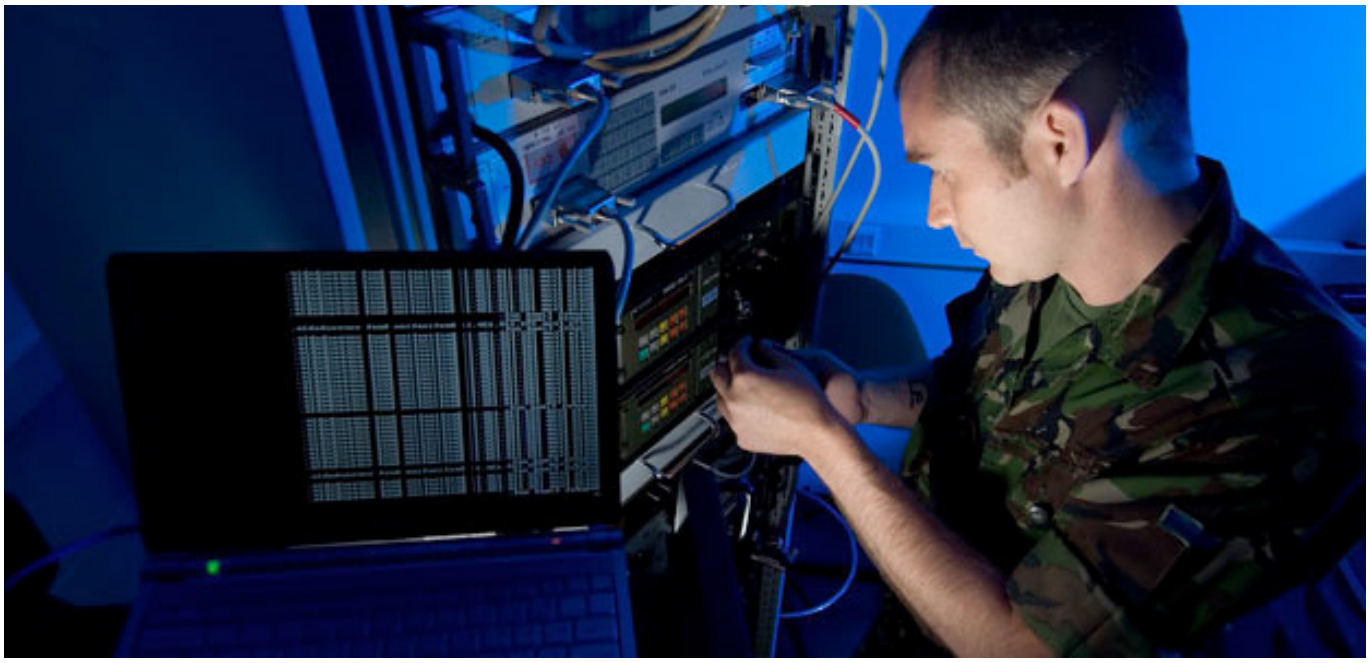
De la misma forma que se creó la Alianza Atlántica en 1949 – para garantizar el apoyo mutuo entre los países firmantes en caso de conflicto – ahora es necesaria una colaboración en el ámbito de la seguridad en el ciberespacio. Desde hace más de una década, todos los países con una madurez elevada en el campo de la ciberseguridad están realizando convenios, programas, colaboraciones e investigaciones conjuntas de gran alcance, realizando formación cruzada e intercambio de expertos. Estas acciones no tienen el carácter internacional que sería deseable y, cada uno de los estados, en función de su soberanía nacional, está decidiendo cual es la mejor forma, de acuerdo a sus propios intereses.

Hay países que invierten o compran empresas en desarrollo con potencial en el campo, como es el caso de Israel. Otros optan por aprender de las organizaciones más avanzadas y con más experiencia en ciberdefensa, como es el caso de Alemania. Algunos otros mejoran las cibercapacidades a través de trabajos conjuntos con la Alianza, como el Reino Unido. En otros casos se realizan programas conjuntos de investigación, como el caso de Arabia Saudí con Estados Unidos, mediante una colaboración entre el KACST y el MIT, o el caso de las multinacionales italianas y francesas en el campo de la ciberseguridad.

Otros países escogen llevar a cabo programas globales conjuntos en ciberdefensa, como es el caso del acuerdo marco entre Francia y el Reino Unido. Algunos otros estados deciden fichar expertos con larga trayectoria en grandes programas de ciberdefensa (muy escasos e insuficientes para cubrir la demanda), como es el caso de los países de Oriente Medio o Asia.

Algunas de estas naciones escogen una combinación de estas opciones, pues su grado de inversión es suficientemente importante como para no dejar cabos sueltos. En este caso, desde el liderazgo político y técnico se coordinan todas estas iniciativas a través de la implantación de programas, como el de ciberseguridad francés, dotado de un presupuesto de mil millones de euros, o el programa británico, dotado con mil doscientos millones de euros.

En estas actividades es vital contar con expertos en una materia que, sin embargo, tiene escasa tradición en la mayoría de los países. Por esa razón, otros países están apostando fuertemente por la captación de estos expertos. Aunque, es cierto, que es necesaria una inversión a futuro adecuada para formar a profesionales en estas competencias. Al final, los esfuerzos en ciberseguridad deben dotarse de un balance equilibrado entre inversiones en personal, en equipamiento, en procesos, en servicios y en sistemas de información. Si este balance no está equilibrado, los programas se ven seriamente afectados.



La demanda de técnicos especializados en ciberseguridad es mucho mayor a la oferta actual disponible en el mercado
Fuente: Biblioteca multimedia de la OTAN

Los analistas de eventos de seguridad tienen que encontrar “la aguja en el pajar”. Saber qué eventos son los relevantes y cuáles no entre millones de ellos, requiere un trabajo previo de inteligencia sobre las ciberamenazas y un gran alto grado de experiencia. El salto cualitativo realizado en Estados Unidos por los ISAC, y en la Alianza Atlántica con sus grandes programas, han convertido a estas organizaciones en la base de la gestión del conocimiento para la gestión de la ciberdefensa.

Es de destacar el esfuerzo realizado por la Alianza Atlántica para incluir a la industria en todo lo relacionado con la ciberseguridad. A finales de año, ésta lanzó el programa OTAN de Asociación en Ciberseguridad con la Industria (NICP) con el fin de aunar esfuerzos e incorporar las innovaciones tecnológicas y la experiencia del sector privado a las iniciativas gubernamentales.

Otros esfuerzos destacables son los relacionados con el Fondo de Confianza en Ciberdefensa OTAN-Ucrania. En este caso, con el liderazgo de Rumanía, países como Albania, Estonia, Hungría, Portugal y Turquía han unido esfuerzos para ayudar a Ucrania a desarrollar capacidades técnicas que le permitan reaccionar a las ciberamenazas, más relacionadas que nunca con sus correspondientes riesgos físicos, dado el clima de tensión que se vive en la zona.

Un analista de eventos de seguridad del Centro de Respuesta a Incidentes de Seguridad de la OTAN (NCIRC) durante su jornada de trabajo
Fuente: OTAN

CONCLUSIONES

Hemos expuesto algunas de las iniciativas de los países y las organizaciones más avanzadas en el ámbito de la ciberdefensa. Cada uno de los países escoge entre varias alternativas para interactuar en un ámbito muy complejo, de la mano, en muchos casos, de organizaciones internacionales y de otras naciones más avanzadas y con un largo recorrido en este campo.

No obstante, también tenemos que afirmar que hay multitud de países que prefieren aún recorrer solos un camino excesivamente complejo, repitiendo errores del pasado, duplicando gastos, invirtiendo en investigaciones ya superadas y que no aportan innovación, en procesos ya implantados y que no funcionan como debieran, en tecnológicas obsoletas, en aplicaciones informáticas desarrolladas a medida cuando ya existen productos que ofrece el propio mercado, que prácticamente cubren todas las capacidades demandadas y que toman otras decisiones que no se apoyan sobre ninguna base, ni aprenden de las experiencias similares del entorno.

"Es fundamental ser creativos e ir un paso por delante en un entorno que se encuentra en cambio constante."

Pensamos que es un error que a largo plazo tendrá consecuencias importantes. Es fundamental ser creativos e ir un paso por delante en un entorno que se encuentra en cambio constante.

También existe otro número de países con un escenario aún más complicado, donde además de afrontar solos una problemática global, llevan a cabo proyectos o programas sin una coordinación común, duplicando multitud de esfuerzos, gastos y objetivos a corto plazo y poco claros. En este marco no se cubrirán a tiempo los criterios mínimos de protección demandados por los ciudadanos.

Abogamos, por un lado, por el establecimiento de lazos de cooperación internacionales y por tomar una inspiración procedente de las iniciativas de otros países para las capacidades de ciberdefensa españolas pero, por otro lado, por generar cuidados procesos y procedimientos de coordinación e intercambio de información entre las distintas entidades del Estado que sean, en mayor o menor medida, responsables de garantizar la ciberseguridad a la sociedad.

Los autores en el Centro de Operaciones del Centro de Respuesta a Incidentes de Seguridad de la OTAN

Finalmente, nos gustaría dejar claro que, en un mercado donde hay una gran demanda de profesionales y un defecto en la oferta, España no debe quedarse atrás en formar personal especializado que pueda llevar a cabo las funciones que se han descrito. Todo ello sin olvidar las inversiones en tecnología propia y en procesos que mejoren la capacidad de reacción ante amenazas a la ciberseguridad.

3 OPINION CIBERELCANO:
Las dos caras de la tecnología

AUTOR: Daniel Sierra, Head of corporate security operations, MAPFRE.
Analista de THIBER, the cybersecurity think tank.

Es una idea comúnmente aceptada el hecho de que los grandes avances de la Civilización se producen o han sido producidos por una idea política o social como motor. Sin duda esa tracción ha sido crucial para el desarrollo de nuestras sociedades a los largo de los siglos. Pero esas ideas sociales no son siempre el origen, sino la consecuencia generada por otra fuerza.

Ahora, con el siglo XXI bien comenzado, parece cada vez los factores motrices de cambio y avance de nuestras sociedades se han reclasificado. La tecnología, en su concepción más amplia, se ha erigido en los últimos tiempos como ese impulso catalizador del progreso, seguidas de ideas las sociales, como consecuencia del cambio de escenario que ha provocado.

Ahora bien, si la tecnología es el motor principal del cambio, ¿qué se puede esperar de este siglo, donde la tecnología está integrada en prácticamente cada actividad humana? Y sobre todo, ¿en qué podemos esperar que afecte a la seguridad?

Esta tecnología está cambiando nuestra manera de relacionarnos, comprar o trabajar. Ante esta situación, cuyas consecuencias a largo plazo apenas vislumbramos aún, es de esperar que se sucedan importantes cambios sociales tal y como ya sucedió con la revolución de la información. El ciberespacio, no sólo no va a ser ajeno a esos cambios, sino que por el contrario va a adquirir un papel protagónico.

La pregunta es obligada, ¿Qué es distinto en el ciberespacio con respecto al mundo tangible? El ciberespacio es el conjunto de medios y procedimientos basados en las tecnologías de la información y la comunicación (TIC) configurados para la prestación de servicios. Está constituido por hardware, software, Internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socio-económica de cualquier estado, en especial aquellos ligados a sus infraestructuras críticas. De esta forma, se infiere que el ciberespacio no es solo internet, ya que internet forma parte del ciberespacio.

La accesibilidad y el bajo coste de los dispositivos de conexión hacen que el ciberespacio crezca exponencialmente, tanto en número de sistemas conectados como de información intercambiada. Esta ambigüedad y complejidad, además de la inmensa cantidad de información manejada, dificulta entender sus constantes cambios. En el ciberespacio además, se desdibujan las fronteras geográficas que condicionan la aplicación del concepto de territorialidad jurídica, concepto básico para la aplicación del derecho, teniendo este hecho, junto con el anonimato en las acciones desarrolladas en el mismo, un efecto drástico en la diplomacia internacional y marcando un nuevo tempo en el desarrollo de conflictos.

La hiperconectividad, el efecto esperado de la globalización, es una realidad. Con conexión permanente a internet y un número ingente (y creciente) de dispositivos conectados y aplicaciones desplegadas, la vida cotidiana es más vulnerable que nunca a las amenazas informáticas y a la indisponibilidad de servicios TIC críticos.

EL CIBERESPACIO EN CIFRAS
Más de 2.300 millones de suscripciones móviles de banda ancha a finales de 2014. Casi 5 veces lo que había en 2008.
Más de 3.000 millones de usuarios de Internet (+ 40% de la población mundial)
Más de 5.000 millones de dispositivos conectados. Se esperan 25.000 millones para 2020.

Fuente: ICT Facts and Figures 2014. ITU

INTERNET EN CIFRAS
14,3 billones de páginas web
672.000.000.000 Gigabytes de información accesible (672 exabytes)
43.639 Petabytes de trafico al año (2013)
1 Yottabyte=10^24 bytes de datos almacenados

Fuente: factshunt

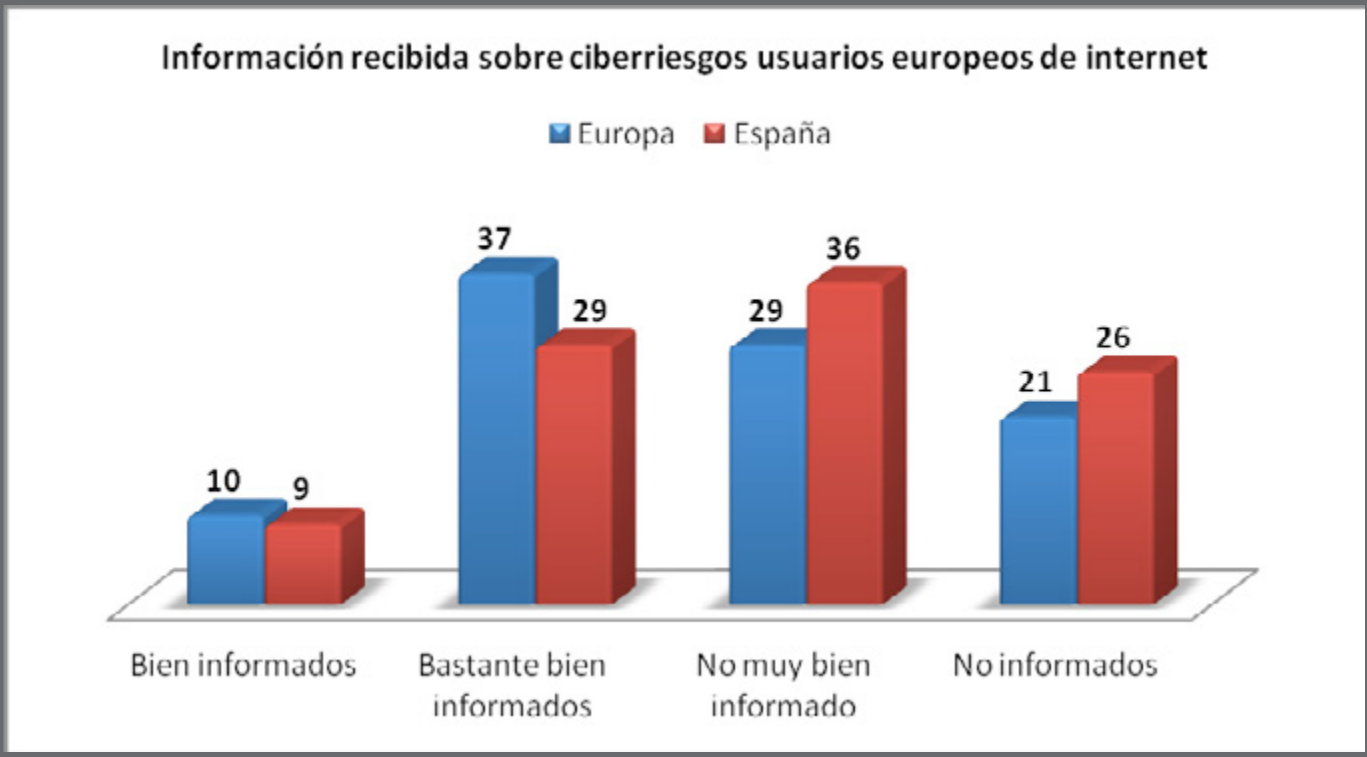
Aquí es donde la tecnología muestra su otra cara: los riesgos inherentes a su uso, que en el caso de las tecnologías de la información son menos conocidos por su reciente incorporación y por sus constantes cambios. Tenemos más facilidad para entender los beneficios de la hiperconectividad que los riesgos asociados.

Ante este situación, cabe preguntarse si realmente ciudadanos, empresas y gobiernos son conscientes de esta situación de riesgo. Los datos del Eurobarómetro desarrollado por Eurostat* a finales de 2014, arrojan una visión sobre la preocupación de los ciudadanos europeos relativos a la ciberseguridad y el cibercrimen.

PREOCUPACIÓN DE LOS USUARIOS EUROPEOS DE INTERNET
89% evitan publicar información personal en Internet
85% consideran que el riesgo de ser víctima del cibercrimen está aumentando
73% tienen preocupación porque su información personal no sea guardada de manera segura por las páginas web
67% tienen preocupación porque su información personal no sea guardada de manera segura por las administraciones públicas

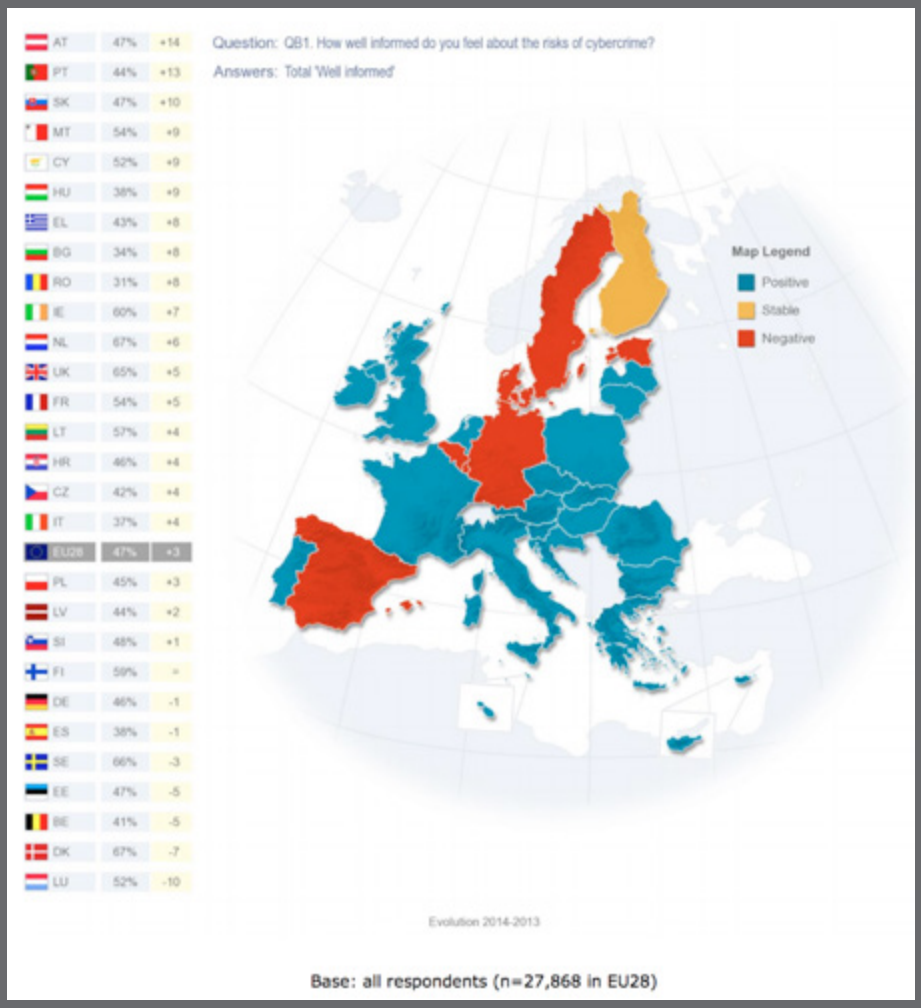
Fuente: *http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf*

Se observa un nivel de preocupación creciente entre la ciudadanía europea, pero la mitad de usuarios consideran que no han sido debidamente informados de los riesgos ligados al ciberespacio.



Fuente: *http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf*

En el caso de España , la cifra alcanza un preocupante 62%, lo cual nos sitúa a la cola en cuanto a nivel de concienciación.



Fuente: *http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf*

Como resultado de esa creciente preocupación, parece que la protección de ciberespacio se ha colado en las agendas políticas de los estados miembro e incluso, tras los atentado de París, se han sentado las bases, mediante la firma de Memorandos de Entendimiento en la plaza europea, clamando por una suerte de Ciberpolítica europea que fije unas reglas básicas éticas de relación y actuación en el ciberespacio, desarrollando el concepto de la ciberdiplomacia (fuente *http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf*)

Pero si la preocupación es creciente, también lo es el riesgo. Casi las tres cuartas partes de las actividades ilegítimas cometidas en el ciberespacio corresponden a alguna variante de cibercrimen, considerada la actividad criminal de mayor crecimiento (cerca de un 175% anual). La realidad muestra que los ciberataques no dejan de aumentar, no sólo en número, sino también en impacto, complejidad, diversificación de objetivos y alcance. El coste aproximado del cibercrimen supera ya la cifra estimada anual de 400.000 millones de dólares con más de 400 millones de víctimas al año (un millón y medio al día), con un número total de incidentes que ronda los 40 millones anuales.

Fuente: PwC Global State of Information Security Survey 2015.

A mayor abundancia, cuanto mayor es la organización, mayor es el coste de un incidente, disparándose un 25% para las para las medianas empresas o un espectacular 52% para las grandes compañías a lo largo de 2014.

Entre el crisol de actividades ilegítimas desarrolladas en el ciberespacio, conviene hacer énfasis en un vector de ataque que es significativamente diferente a los demás. Normalmente los ataques son puntuales, sin extenderse en el tiempo,. Ya sea la mera modificación del contenido de una página web, una denegación de servicio o una penetración en un sistema o red para obtener información, los ciberdelincuentes consiguen acceso, provocan el daño, y se retiran.

Sin embargo, existen otros ataques, potencialmente dirigidos y focalizados, cuyo principal valor es el acceso persistente en el tiempo a las redes y equipos de sus objetivos. Este tipo de ataques, son denominados comúnmente amenazas persistentes avanzadas (APT, por sus siglas en inglés). Las APTs son un conjunto de procesos de ataque, ocultos y continuos en el tiempo, con un objetivo específico, normalmente por motivos económicos o políticos/estratégicos. En su génesis, debido a la complejidad técnica que revestían y la selección de objetivos, su autoría ha sido atribuida a actores estatales con grandes recursos materiales. Sin embargo, este tipo de técnicas han sido paulatinamente adoptadas por grupos organizados han comenzado a liderar campañas de este tipo.

Es ahora cuando la industria de la ciberseguridad comienza a detectar estos vectores de ataque, muchos de ellos operativos desde hace más de un lustro. A modo ilustrativo, una de estas operaciones, llamada Carnabank, diseñada para sustraer dinero de cuentas bancarias, ya ha incautado más de 1000 millones de dólares a varios bancos, siendo considerada una de las actuaciones de su naturaleza más rentable hasta la fecha. Fue descubierta en 2014 y, hasta donde se ha podido analizar, se encontraba operativa desde 2013. Otra de ellas, denominada Dark Hotel , permitía a espiar y sustraer información a personalidades VIP en hoteles por todo el mundo.

De nuevo, fue descubierta en 2014, pero se tienen registros de actividad desde 2007. Este tiempo delta existente entre la detección de estas operaciones de complejidad exponencial y el momento desde el cual comenzaron a activarse, supone un nivel temporal de exposición para los objetivos enorme.

Es previsible una escalada armamentística en el ciberespacio, pues a medida que avanza su desarrollo, cada vez los conocimientos necesarios y el riesgo de usarlos son y serán menores. Del mismo modo que ocurrió con las armas tradicionales, la evolución del de la espada, al rifle, al cañón y al misil, supuso un aumento exponencial en capacidad destructiva.

Para aproximar la solución al problema, dada su complejidad, es necesario un esfuerzo común de todos los estamentos implicados. Ciertamente un marco legislativo punitivo y con presupuesto asignado, es la primera piedra a colocar, y en eso ya se está trabajando. Pero es necesario complementarlo con un marco incentivador, de forma que se estimule la adopción de mejores prácticas en ciberseguridad, como se ha desarrollado por ejemplo en Israel, con un éxito rotundo, donde el centro de referencia de ciberseguridad, ha acabado siendo también prolífica cuna de multitud de nuevas empresas tecnológicas.

Pero las empresas y los ciudadanos también tienen que dar pasos que nos encaminen en la dirección deseada, que no es otra que reducir los riesgos. Los ciudadanos pueden aumentar el nivel de exigencia, no sólo a sus gobiernos, sino también a los fabricantes del hardware y software que utilizan, de modo que estos tengan unos niveles mínimos de seguridad, como ya hacen con otras sectores industriales (¿quién se compraría un coche sin cinturón de seguridad o cuyas puertas no se cerrasen con una llave?). También debemos ser conscientes de que nuestro nivel de exposición en el ciberespacio. A este respecto, utilizar servicios gratis aunque convenientes, no ayuda porque en realidad en ellos, los usuarios no son los clientes y por tanto no pueden presionar al proveedor. Los usuarios (sus datos) son el producto, y cualquiera que utilice una de esas plataformas debe aceptar que lo que publique ahí escapara casi seguro a su control. Y las empresas y los emprendedores, deben aprovechar el momentum de la industria, y aprovechar la situación para crear nuevos productos y servicios que la sociedad demanda cada vez más.

No se abandona una tecnología útil porque su uso implique gestionar o asumir ciertos riesgos, pues éstos siempre existirán, pero es importante identificarlos para poder estar preparados. Es una responsabilidad compartida.

4 Entrevista a GD. Carlos Gómez López de Medina

Comandante Jefe del Mando Conjunto de Ciberdefensa (MCCD)

1. ¿Podría explicar brevemente cuál es la función del Mando Conjunto de Ciberdefensa (MCCD)?

Tal y como nos muestran las operaciones militares recientes, las fuerzas armadas modernas son muy dependientes del ciberespacio para operar eficazmente. Además, el ciberespacio no sólo es un habilitador de las operaciones militares terrestres, navales, aéreas y espaciales; sino que también se ha convertido en un dominio en el que operar.

Teniendo en cuenta estos elementos, es vital que exista un Mando como el nuestro, el MCCD. En este sentido, tal y como establece la *Orden de Defensa 166/2015*, del pasado 21 de enero, el MCCD dirige y coordina – en materia de ciberdefensa – la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos. Ejerce la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. Define, dirige y coordina la concienciación, la formación y el adiestramiento especializado en esta materia. Además, será responsable del desarrollo y detalle de las políticas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones y de la dirección de la ejecución y el control del cumplimiento de estas políticas, en el ámbito del Ministerio de Defensa. Finalmente, nuestro ámbito de actuación son las redes y los sistemas de información del Ministerio de Defensa, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional.

2. ¿Cómo se integra el MCCD en el marco del Sistema de Ciberseguridad Nacional?

El MCCD nació al mismo tiempo que se redactaba la Estrategia Nacional de Ciberseguridad (ENCS), lo que facilitó la inclusión del propio MCCD en la Estrategia. Además, la integración práctica se realiza mediante nuestra participación – el Comandante del MCCD es el vocal del Ministerio de Defensa – en el Consejo Nacional de Ciberseguridad (CNCS), un foro en el que están representados buena parte de los ministerios del gobierno de la nación, así como el Centro Nacional de Inteligencia y el Departamento de Seguridad Nacional. Éste último asume también la Secretaría del CNCS, proporciona coordinación con los demás Comités Especializados y facilita la relación con el Consejo de Seguridad Nacional. El CNCS va a aumentar la velocidad de progresión en nuestras capacidades de ciberseguridad a nivel nacional. Su creación ha sido un gran acierto. Cuando comentamos nuestras experiencias con fuerzas armadas de naciones aliadas, siempre resaltamos la gran ventaja que supone disponer de un organismo coordinador de ese nivel.

3. Centrándonos más en los asuntos de defensa, ¿cómo definiría la ciberdefensa?

La ciberdefensa no sólo la entendemos en su vertiente defensiva ya que nosotros barajamos las capacidades de defensa, de explotación y también de respuesta, esto es, ofensivas. En otras palabras, la capacidad de defensa está vinculada con la ciberseguridad y en esta actividad tenemos muchas similitudes con otros organismos, instituciones y empresas que necesitan ser "ciberseguros". Lógicamente, en materia de explotación y de respuesta no tenemos tantos "compañeros de viaje".

Es necesario proporcionar capacidades de ciberdefensa a las Fuerzas Armadas porque es evidente que los potenciales agresores son estados o grupos organizados con capacidades muy sofisticadas. Es por ello que no sólo debemos protegernos y ser resilientes a los ataques, sino también generar capacidades ofensivas que nos permitan responder a los mismos.

4. En base a su concepción acerca de la ciberdefensa, cuáles son las capacidades que el Mando está generando? ¿Defensivas, ofensivas, explotación?

Estamos desarrollando las tres capacidades en paralelo, pero su desarrollo no se realiza a la misma velocidad. En este sentido, aunque podemos afirmar que tenemos capacidades en las tres áreas, hemos "apretado más el acelerador" en las capacidades defensivas.

Además, ya proporcionamos capacidades de ciberdefensa a todo el Ministerio de Defensa y no sólo a las Fuerzas Armadas. Y es que si bien los Ejércitos y la Armada son responsables de sus sistemas específicos, el MCCD es responsable de los sistemas conjuntos. En otras palabras, estamos avanzando satisfactoriamente.

"ya proporcionamos capacidades de ciberdefensa a todo el Ministerio de Defensa y no sólo a las Fuerzas Armadas."

5. Han pasado dos años desde la constitución del MCCD. ¿Podría hacer una breve evaluación de los hitos alcanzados?

El MCCD se creó con la *Orden Ministerial 10/2013* del 19 Febrero de 2013 y pocos meses después, más concretamente el 27 de Septiembre del mismo año, ya logramos la Capacidad Operativa Inicial. Desde entonces, hemos realizado importantes progresos y hemos desarrollado muchas capacidades, y todo ello gracias a nuestros recursos humanos y materiales. Nuestro objetivo a corto plazo es lograr la Plena Capacidad Operativa.

Hemos desarrollado un plan de formación que, denominado FORCIBE, pretende educar y formar al personal de las Fuerzas Armadas en materia de ciberdefensa a todos los niveles, desde las academias militares y cursos de perfeccionamiento a los cursos de Altos Estudios Militares. Más concretamente, el plan FORCIBE se plasmará, cuando se lance en el curso 2015-16, en la elaboración de tres tipos de enseñanzas – básicas, avanzadas y especializadas – realizadas a nivel conjunto de las Fuerzas Armadas. El Plan FORCIBE ha podido desarrollarse gracias a la colaboración generosa y entusiasta de todos los Organismos implicados: Ejércitos, Armada, Órgano Central del Ministerio y Estado Mayor de la Defensa.

"Hemos desarrollado FORCIBE, para educar y formar al personal de las FAS en materia de ciberdefensa"

Y mientras el plan FORCIBE no comienza su andadura, nuestra formación en materia de ciberdefensa se realiza principalmente a través de los cursos proporcionados por el Centro Criptológico Nacional (CCN) y el Centro de Excelencia en Ciberseguridad de la Alianza Atlántica (*CCD-CoE* en Tallin, Estonia), pero siempre atendiendo a los perfiles de personal que buscamos en el MCCD. Además, si esta formación no satisface nuestras necesidades, también contratamos cursos ad hoc con profesionales de referencia o con empresas que dispongan de los conocimientos específicos en la materia. En España contamos con muy buenos profesionales de la ciberseguridad.

6. ¿Nos podría decir si ya se están planteando operaciones españolas en el ciberespacio?

Sin ningún tipo de duda. De hecho, dentro de la estructura de la Fuerza Conjunta, el MCCD es el quinto Mando Componente (Mando Componente Ciber). Esta Fuerza Conjunta está a disposición del Jefe de Estado Mayor de la Defensa (JEMAD) y su jefatura la ostenta el Comandante del Mando de Operaciones (CMOPS), que cuando planea lo hace con las capacidades terrestres, navales, aéreas, de operaciones especiales y las nuestras, las cibernéticas. En consecuencia, nosotros participamos en el planeamiento y la conducción de la operación. Además, hay que resaltar que la defensa del ciberespacio de nuestra responsabilidad tiene carácter de misión permanente.

7. Siempre se comenta que uno de los mayores activos de las Fuerzas Armadas es el personal, en este sentido, ¿Nos podría explicar brevemente los perfiles del personal que está destinado en este mando?

En el MCCD disponemos de personal militar de los Ejércitos y la Armada con formación y experiencia en las Tecnologías de la Información y las Comunicaciones, muchos de ellos también tenían experiencia en ciberdefensa cuando llegaron al MCCD. Asimismo, contamos con el apoyo proporcionado por ISDEFE (ingenieros informáticos y de telecomunicaciones con experiencia en ciberdefensa). También estamos muy próximos a incorporar funcionarios civiles TIC (Grupo A, titulados también en ingeniería informática o telecomunicaciones). Actualmente, el MCCD lo integramos setenta personas, pero este número va a seguir creciendo de forma importante.

8. Francia y Reino Unido están destinando muchos recursos para el desarrollo de su ciberdefensa ¿Cómo estamos en comparación con nuestros aliados?

Cualquier comparativa debemos realizarla a nivel nacional, puesto que la inversión en recursos la realiza todo el país. De hecho, si sumáramos los recursos económicos y humanos de todos los integrantes del Sistema Nacional de Ciberseguridad – y no sólo el MCCD – obtendríamos una cantidad nada desdeñable. Además, estoy convencido de que nuestra asignación de recursos crecerá cada vez más.

No obstante, es importante tener en cuenta que antes de disponer de grandes recursos económicos, hay que contar con una organización bien estructurada para poder ser eficaces y eficientes. Este es un requisito imprescindible para obtener el máximo de las inversiones realizadas. Personalmente creo que ahora se está construyendo esa organización a nivel nacional y en cada uno de los Ministerios, lo mismo que lo estamos haciendo nosotros en el Ministerio de Defensa.

9. Tal y como plantea la Estrategia de Seguridad Nacional, el ciberespacio es un nuevo dominio. ¿Cree que todos los actores, tanto públicos como privados, han observado la importancia de este dominio?

Somos cada vez más conscientes de ello, aunque también es cierto que queda mucho por hacer. De hecho, una de las líneas de acción de la *Estrategia Nacional de Ciberseguridad* tiene por objeto "aumentar la cultura de ciberseguridad". Es, por lo tanto, imprescindible realizar una labor de concienciación a todos los niveles, ya que cualquier ciudadano, organismo, institución y empresa está afectado por lo que sucede en el ciberespacio.

5 Informes y análisis sobre ciberseguridad publicados en Marzo de 2015

Eurobarometer: Cyber Security Report (European Commission)

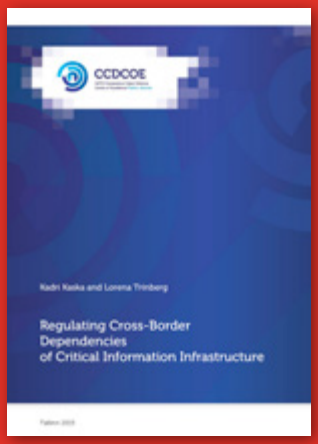
Council of the European Union conclusions on Cyber Diplomacy (Council of the European Union)

The role of Insurance in managing and mitigating the risk (UK Government and MARSH)

Small Businesses: What you need to know about cybersecurity (UK Government)

National/ Governmental CERTs, recommendations on baseline capabilities (ENISA)

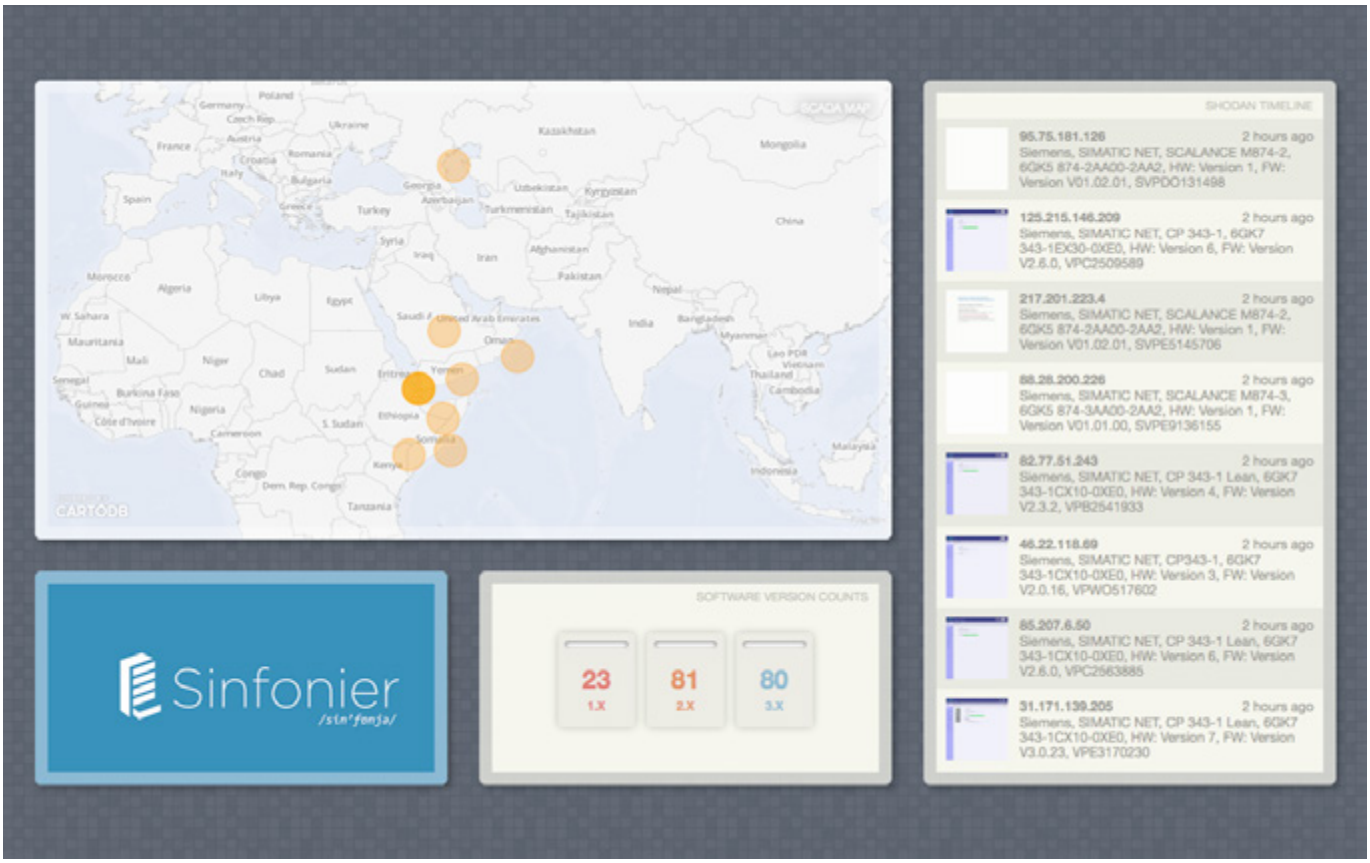
Regulating Cross-Border dependencies of Critical Information Infrestructure (CCD COE)



Cyber Threat Information Sharing – Recommendations for Congress and Administration (CSIS)

Cyber Red Teaming: Organizational, technical and legal implications in the military context (CCD COE)

6 Herramientas del analista: SINFONIER



El ciberespacio, con un volumen de información intercambiada y procesada superior a los 50.000 Petabytes al año, supone un cambio de paradigma para los analistas de inteligencia. Si en el pasado el problema era la recopilación de información, ahora el analista se enfrenta a la infotoxicidad o saturación de datos y a la necesidad de procesarlos y analizarlos generando inteligencia en tiempo real.

Sinfonier es una herramienta que permite utilizar tecnología de procesamiento de datos (Apache Storm) de forma sencilla e intuitiva. Además es española y gratuita, impulsada por Telefonica, nacida con el propósito de convertirse en una comunidad para desarrolladores e investigadores del ámbito de la seguridad.

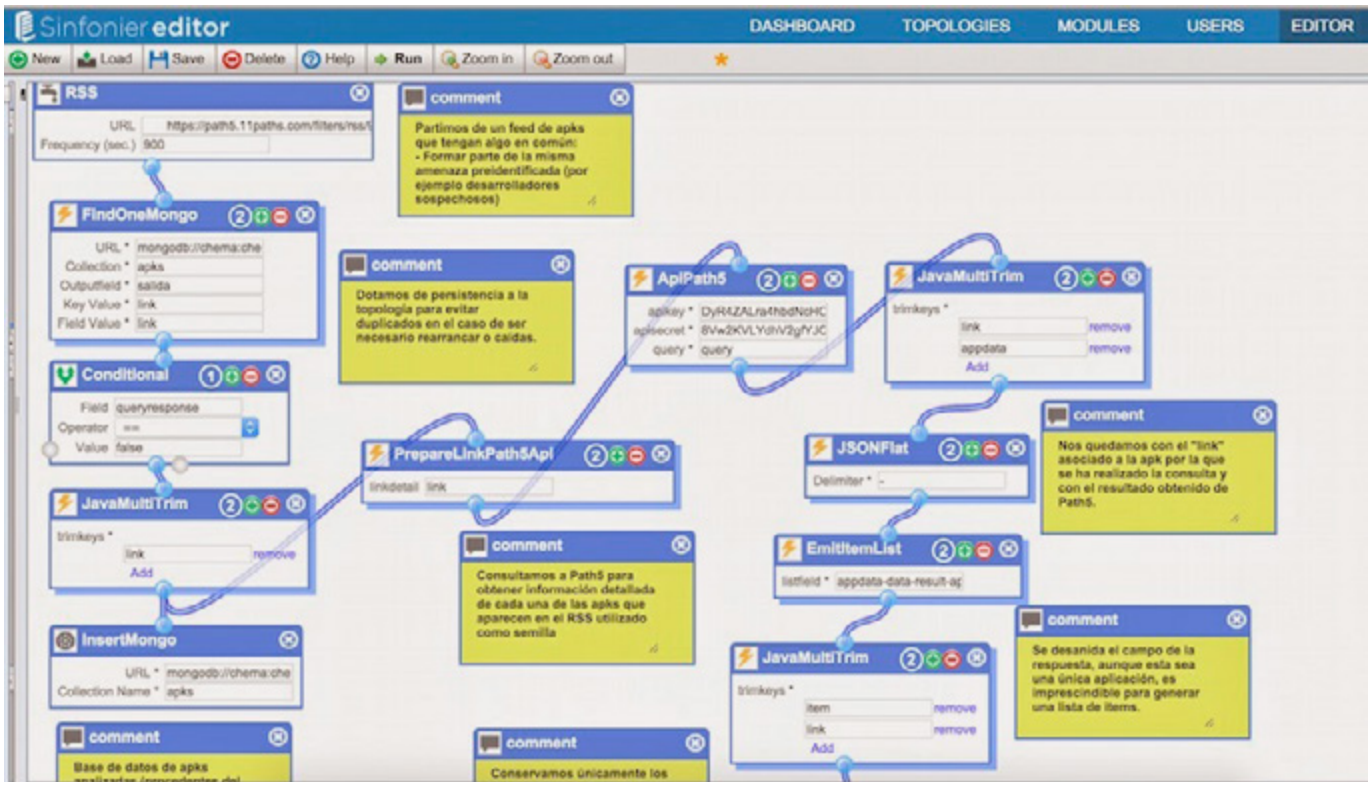
El objetivo principal de Sinfonier es facilitar el proceso de generación de inteligencia a través de un modelo colaborativo en el que los desarrolladores generan módulos que permiten conectar Sinfonier con interfaces para la obtención, transformación y almacenamiento o envío a sistemas de visualización de la información para que de forma posterior, sean utilizados por toda la comunidad para generar sus propios algoritmos de inteligencia.

Sinfonier combina un entorno colaborativo y de desarrollo sencillo con un interfaz amigable que permite definir nuevos algoritmos con un lenguaje de programación visual basado en “arrastrar y soltar módulos” (drag&drop).

El resultado de Sinfonier es una comunidad de conocimiento y cooperación donde el trabajo puede ser reutilizado y los esfuerzos puestos en mejorar el procesamiento y recolección de la nueva información que se va generando.

Desde investigadores sin conocimientos de programación y desarrolladores con amplia experiencia programando hasta medianas y grandes empresas pueden utilizar Sinfonier como herramienta para el procesamiento y enriquecimiento de información con el objetivo de conseguir crear nueva información integrando Sinfonier en su proceso de inteligencia.

Sinfonier pone a disposición de sus usuarios la capacidad para recolectar información desde multitud de fuentes, procesarla y enriquecerla de forma dinámica y continua. Son los usuarios los que tendrán que proveer de contenido los algoritmos en forma de topologías y sacar el máximo partido a dicha información.



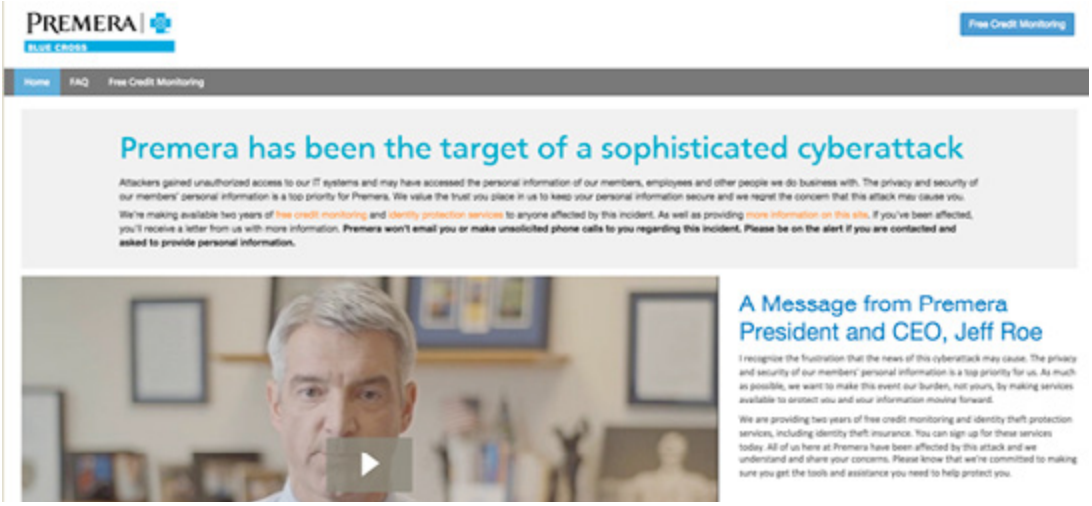
“Sinfonier pone a disposición de los usuarios la capacidad para recolectar información desde multitud de fuentes, procesarla y enriquecerla de forma dinámica y continua”

7 Análisis de los ciberataques del mes de marzo de 2015

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

Durante el mes de marzo se ha registrado un nivel de actividad menor de acciones ilegítimas en el ciberespacio.

Por una parte, el FBI está investigando el reciente ciberataque desarrollado contra Empire Blue Cross Blue Shield, la compañía de seguros cuya matriz es Anthem Inc, segunda aseguradora sanitaria norteamericana objeto también de una fuga masiva de datos a comienzos de año afectando a más de 80 millones de usuarios.

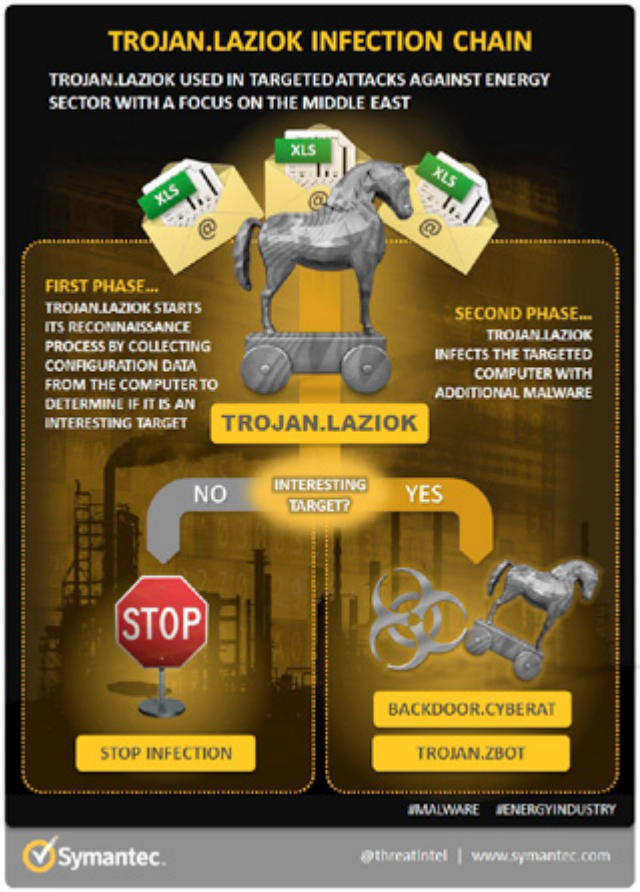


GitHub una de las principales forjas para alojar proyectos de desarrollo utilizando el sistema de control de versiones Git, fue afectado por un ataque de denegación de servicio distribuido (DDoS). Algunos analistas apuntan a China como responsable material, identificando diversas IPs de ese país como origen del tráfico que inundó los servidores de **GitHub.**

Por su parte, mientras los medios de comunicación se hacían eco del accidente aéreo de GermanWings, miles de cuentas de viajeros frecuentes del esquema de fidelización de **British Airways** fueron filtradas, identificándose usos fraudulentos de la información de los usuarios asociados (reservas hoteleras, cargos a las tarjetas de crédito vinculadas, etc.).

Entre las actividades hacktivistas de origen religioso y político, se ha detectado una importante escalada de ataques de defacement por parte los grupos favorables al Daesh sobre multitud de webs europeas y norteamericanas. Por su parte, **Anonghost**, colectivo pro-palestino, protagonizó diversas operaciones sobre objetivos estadounidenses e israelíes. **Anonymous mostró un repunte en sus actividades.**

A finales de mes, analistas de la firma Symantec hicieron público el descubrimiento de Trojan. Laziok, una nueva muestra de malware dirigido a empresas del sector energético de todo el mundo, cuyo nivel de sofisticación y el elenco de objetivos apunta a un actor estatal como promotor del mismo. Con especial énfasis en las industrias petrolera y gasística de Oriente Medio, también ha afectado a países como Camerún, Colombia, India, Indonesia, Kuwait, Omán, Pakistán, Qatar, Arabia Saudí, Uganda, Emiratos Árabes Unidos, Reino Unido y Estados Unidos.



En el plano nacional, se han detectado diversas campañas de phising, como el que ha afectado a los clientes de diversas entidades financieras como **la Caixa**, así como una campaña focalizada en el popular servicio de mensajería **WhatsApp** y su nueva funcionalidad de llamada embebida, o las ya habituales campañas estacionales que explotan el periodo de presentación de las Declaraciones de Renta, **suplantando la identidad de la Agencia Tributaria.**

Adicionalmente, hemos asistido a la proliferación durante el mes de marzo de dos nuevas cepas de ransomware, presentando cierta similitud con el esquema del conocido **Cryptolocker** o TorrentLocker, que afectó a multitud de usuarios y empresas españolas hace tan solo unos meses. **Cryptofortress**, similar a TorrentLocker, y **Teslacrypt**, un malware cuya principal peculiaridad se encuentra en la naturaleza de los archivos que cifra puesto que entre ellos se encuentran algunos pertenecientes a videojuegos muy populares."

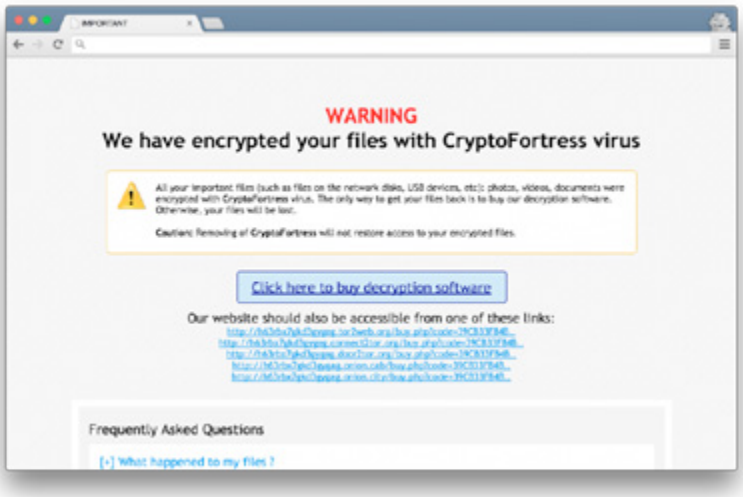
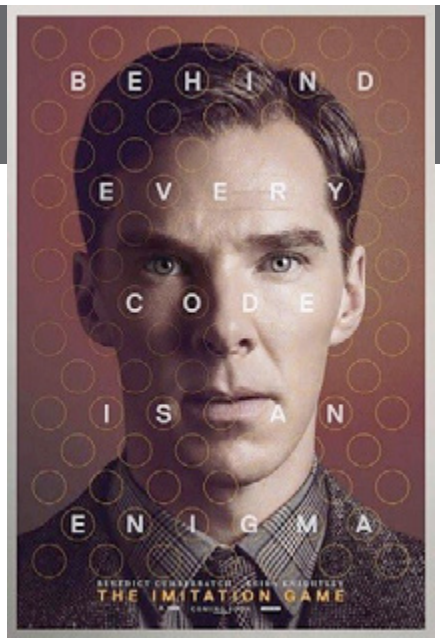


Ilustración 1 Mensaje arrojado por CryptoFortress

8 Recomendaciones

8.1 Libros y películas

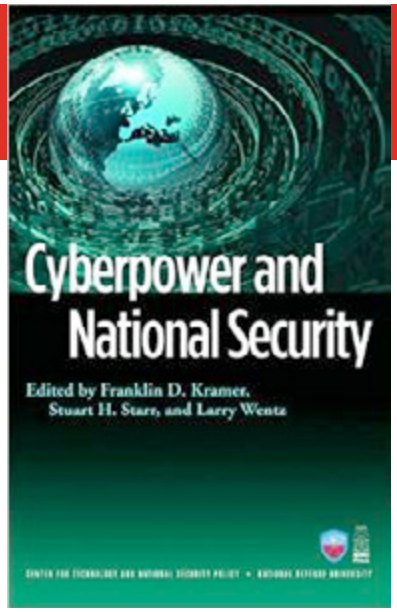


Película:
THE IMITATION GAME (Descifrando Enigma)

Sinopsis: Biopic sobre el matemático británico Alan Turing, famoso por haber descifrado los códigos secretos nazis contenidos en la máquina Enigma, lo cual determinó el devenir de la II Guerra Mundial (1939-1945) en favor de los Aliados. Lejos de ser admirado como un héroe, Turing fue acusado y juzgado por su condición de homosexual en 1952.

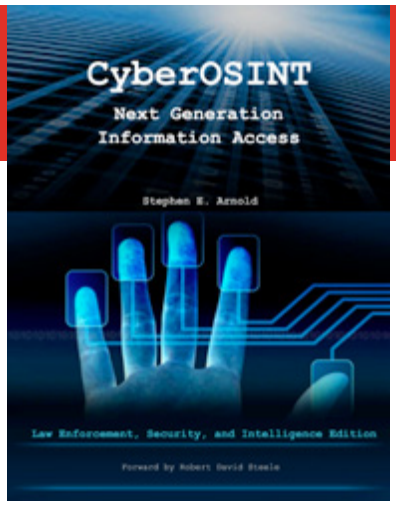
Película:
CITIZEN FOUR

Sinopsis: En enero de 2013, Laura Poitras comenzó a recibir correos electrónicos cifrados firmados por un individuo que se autodenomina “Citizenfour”, en los que le aseguraba tener pruebas de los programas de vigilancia ilegales dirigidos por la NSA en colaboración con otras agencias de inteligencia en todo el mundo. Cinco meses más tarde, junto con los periodistas Glenn Greenwald y Ewen MacAskill voló a Hong Kong para fijar el primero de muchos encuentros con un hombre anónimo que resultó ser Edward Snowden. En sus encuentros, viajó siempre con una cámara. La película resultante es la historia que se desarrolla ante nuestros ojos en este documental galardonado con un Oscar al mejor documental en 2015.



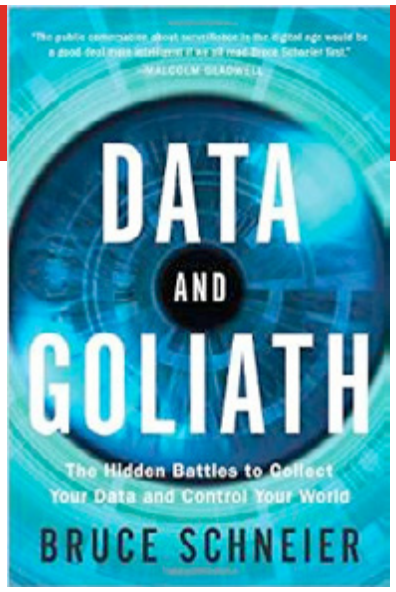
Libro:
BERPOWER AND NATIONAL SECURITY

Autor: Fanklin Kramer, Stuart Star, Larry Wentz
Num. Paginas: 600
Editorial: Potomac Books Inc
Año: 2009
Precio: 20.00 Euros
Sinopsis: El ciberespacio se ha convertido en el quinto dominio del campo de batalla. Este hecho no solo supone una gran oportunidad para las Fuerzas Armadas modernas sino también una de sus principales amenazas. Este libro se adentra de un modo singular en el mundo de las ciberoperaciones militares.



Libro:
CYBEROSINT: NEXT-GENERATION INFORMATION ACCESS

Autor: Stephen Arnold
Num. Paginas: 178
Editorial: Xenky
Año: Abril 2015
Precio: 45 Euros
Sinopsis: Esta obra recopila las principales capacidades tecnológicas de ultima generación esenciales para cualquier analista involucrado en el trabajo de investigación, las operaciones militares y actividades de inteligencia en el ciberespacio.



Libro:
DATA AND GOLIATH

Autor: Bruce Schneier
Num. Paginas: 400
Editorial: W.W. Norton & Company
Año: Abril 2015
Precio: 19.65 Euros
Sinopsis: Bruce Schneier, uno de los principales gurús internacionales en el ámbito de la ciberseguridad, nos explica como los gobiernos hacen uso delos datos que fluyen por Internet para aumentar sus actividades de vigilancia, censura y propaganda.

8.2 Webs recomendadas

https://ccdcoe.org/
El Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE) es un centro internacional al servicio de la OTAN que tiene por misión la investigación y la formación en materia de ciberdefensa.

https://www.cci-es.org/
El CCI es un referente nacional e internacional en el ámbito de la ciberseguridad de las organizaciones e infraestructuras industriales.

http://www.emad.mde.es/CIBERDEFENSA/
Es el sitio web del Mando Conjunto de Ciberdefensa. Para mas información consultar la entrevista que publicamos en el presente numero con su Comandante Jefe, el GD. Carlos Gómez López de Medina.

http://www.elladodelmal.com/
Un informático en el lado del mal es el canal de publicación de los artículos diarios sobre seguridad de la información publicados por Chema Alonso.

http://www.darkreading.com/
Dark Reading es uno de los sitios webs mas leidos en materia de seguridad informática. Su enfoque multi-disciplinar le permite a glutinar a la inmensa mayoría de los principales profesionales del sector.

https://www.ismsforum.es/
ISMS Forum Spain, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España.

8.3 Cuentas de Twitter

@ccdcoe

@cyber

@threatpost

@enisa_eu

@CyberEssentials

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
09-abr	Madrid	UPM TASSI	Quinta conferencia del XI Ciclo de Conferencias UPM TASSI	http://www.lpsi.eui.upm.es/GANLESI/2014_2015/gconferencia_jmm.htm
09-abr	Amadora (Portugal)	The Ministry of Defence of Portugal (MDN), NATO Industry Cyber Partnership (NICP), CIIWA and AFCEA Portugal	1st NATO Cyber Defence Smart Defence Projects' Conference	http://www.mncdet-pt.net/#!1st-NATO-CD-SDP-Conference/cf1c/EventListItem2_i5o2u4pu5_2
10-11 abril	Córdoba	Qurtuba	Qurtuba Security Congress	http://qurtuba.es/
14-17abril	Singapur	a-Star / ADSC	1st Cyber-Physical System Security Workshop CPSS 2015	http://icsd.i2r.a-star.edu.sg/cpss15/
14-abr	Madrid	Fundación Consejo España - EEUU, RIElcano, Aspen Institute y la Embajada de USA	"ESPAÑA Y ESTADOS UNIDOS ANTE LOS DESAFÍOS DE LA CIBERSEGURIDAD".	http://www.spainusa.org/es/eventos/espana-y-estados-unidos-ante-los-desafios-de-la-ciberseguridad
14-16 abril	Marsella	SAFIM	AccessSecurity	http://accessecurity.fr/
13-16 abril	Moscú	MIPS	MIPS Moscow	http://www.mips.ru/en-GB
21-23 abril	Ciudad de México	Expo tecnología	Expo Tecnología TIC's y Seguridad	http://expo-tecnologia.com
21-23 abril	Madrid	Revista SIC	Securmatica 2015	http://www.securmatica.com/
28-29 abril	Madrid	Mundo Hacker	Mundo Hacker day 2015	http://www.mundohackerday.com/
20-24 abril	San Francisco	RSA	RSA Conference 2015	http://www.rsaconference.com/events/us15
20-may	Madrid	ISMS Forum	XVII ISMS Forum Spain	https://www.ismsforum.es/noticias/noticia.php?idnoticia=610

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