MARZO 2015 / Nº 1

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 Informes y análisis sobre ciberseguridad publicados en Febrero de 2015 04

2 Herramientas del analista 06

3 Timeline de ciberataques 07

4 El ciberespacio como campo de batalla. 08

5 ANÁLISIS DE ACTUALIDAD INTERNACIONAL: La esquizofrénica diplomacia pública de los ayatolás 10

6 Estrategias nacionales de ciberseguridad en el mundo 16

7 Entrevista a Joaquín Castellón 17

8 Recomendaciones

8.1 Libros y películas 21

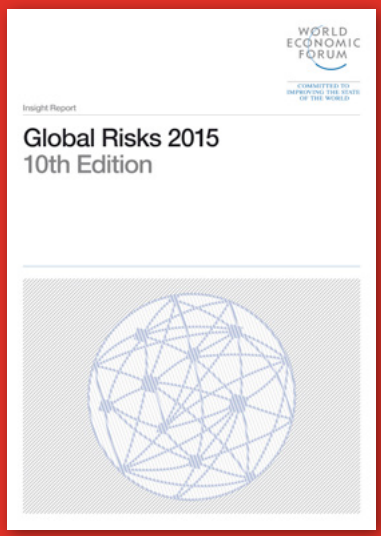
8.2 Webs recomendadas 23

8.3 Cuentas de Twitter 24

9 Eventos 25

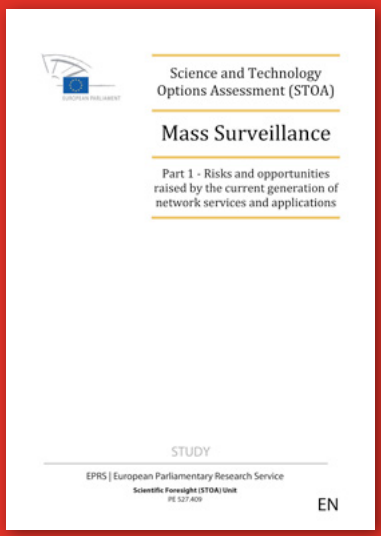
1 Informes y análisis sobre ciberseguridad publicados en Febrero de 2015

The Global Risks 2015 (World Economic Forum)

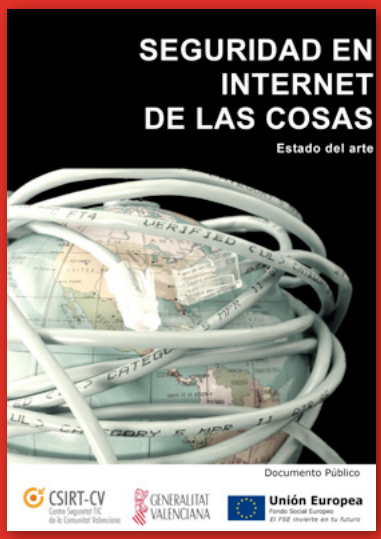


Behind the syrian conflict's digital front lines. Fireeye threat intelligence.

Vigilancia Masiva (Parlamento Europeo)

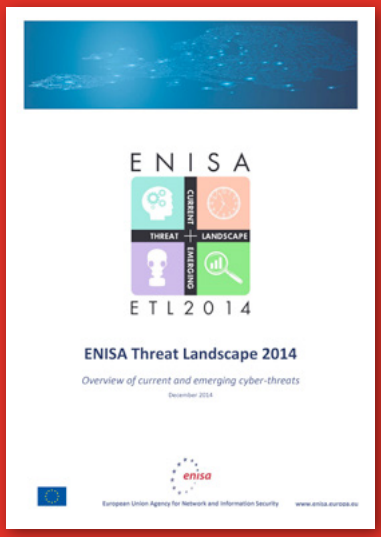


Seguridad en Internet de las cosas (CSIRTCV - Parlamento Europeo)

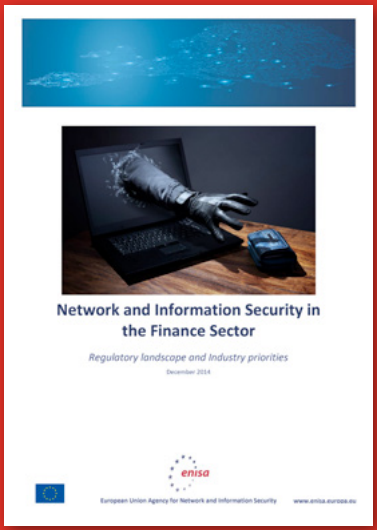


Challenges at the intersection of Cyber Security and Space Security (Chatam House)

ENISA Threat Landscape 2014 (ENISA)

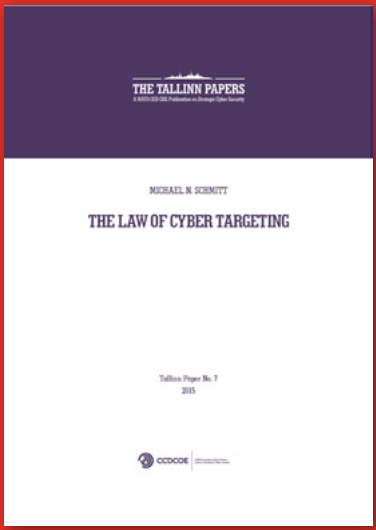


Network and Information Security in the Finance Sector (ENISA)



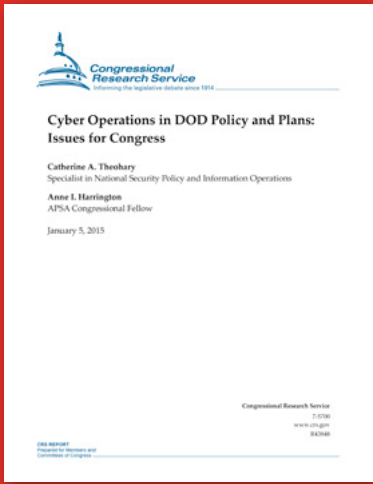
Privacy and Data Protection by Design (ENISA)

The law of cyber targeting (CCD COE)



US – UK Cybersecurity Cooperation (White House)

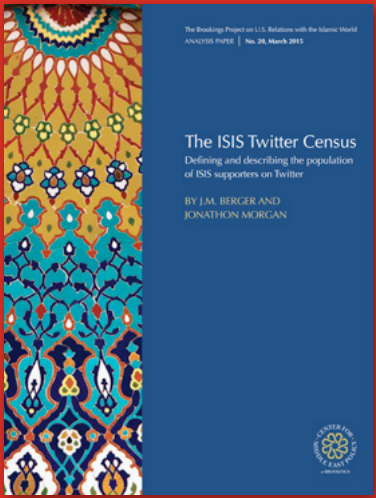
Cyber Operations in DoD Policy and Plans : Issues for Congress (U.S Congress)



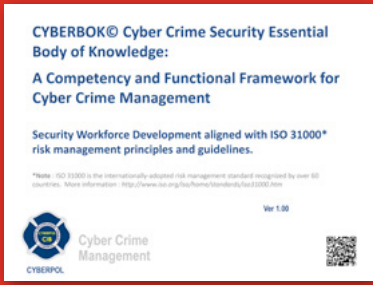
CISCO 2014 Annual Security Report (CISCO)

Cyber Resilience: a financial stability perspective (Bank of England)

The ISIS Twitter Census (Brooking)



Cyber Crime Security Essential Body of Knowledge (CYBERPOL)



2 Herramientas del analista

Personal del centro de operaciones de la Unidad de Comando Cibernético estadounidense, en la base de San Antonio, Tejas. FUERZAS AÉREAS DE EE UU. Fuente: EL PAIS

DSHELL: el software open source de ciberseguridad de la armada estadounidense

https://github.com/USArmyResearchLab/Dshell

El Ejército de Estados Unidos ha compartido un programa open source utilizado para analizar los ciberataques. Desde hace cinco años, cada vez que una red del Departamento de Defensa ha estado en peligro, el Ejército ha utilizado el marco DSHELL para ejecutar análisis forense sobre los ataques. Esta medida tiene la intención de animar a los programadores a añadir módulos personalizados que va a ayudar al ejército a entender lo que sucede cuando son atacados.

3 Timeline de ciberataques

Bajo estas líneas se muestra un timeline de los principales ciberataques identificados enero y febrero de 2015, elaborados por Paolo Passeri (@PaulSparrows) en su web hackmageddon.com. Tras los atentados sucedidos en París el 14 de enero de 2015 a la editorial del 'Charlie Hebdo', cuya autor.a intelectual fue reclamada a través de un comunicado online por Harez al Dari, supuesto líder de la rama yemení de Al Qaeda, se observa un número de ciberataques sin precedentes (cerca de 19.000) sobre infraestructuras tecnológicas francesas, potencialmente provenientes de hackers pro-islamistas.

Anonymous, por su parte, protagonizó una campaña contra el Daesh, teniendo como punto focal diversos sites yihadistas. Al mismo tiempo algunas de las cuentas en redes sociales del US CENTCOM fueron también atacadas.

El ciberataque masivo desarrollado contra la segunda aseguradora estadounidense Anthem, afectando a más de 80 millones de registros, y la sofisticación de la campaña Operation Carnabak que ha tenido como consencuencia el robo de 300 M$ en 100 bancos a lo largo de 30 países han sido los actores protagónicos en la primera quincena del mes de febrero.

En el plano de los ataques persistentes avanzados, el marco de ciberoperaciones desarrolladas por The Equation Group han fijado un nuevo hito en términos de sofisticación, llevando presentes más de una década.

El timeline de los principales ciberataques de febrero de 2015 clasificados quincenalmente pueden consultarse aquí y aquí.

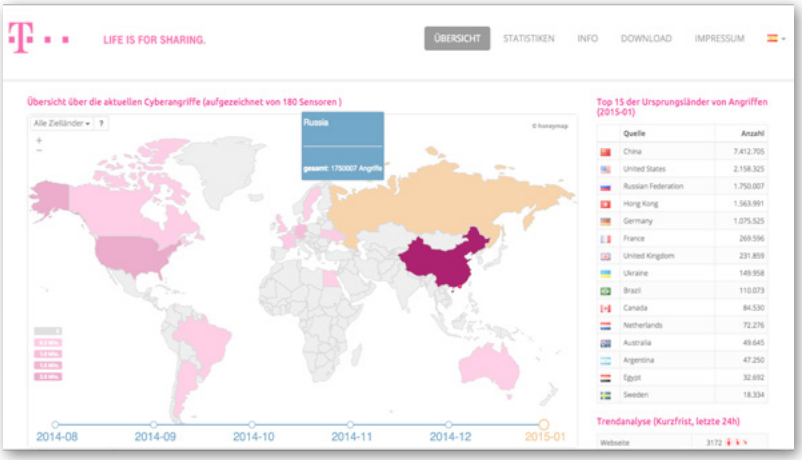
4 El ciberespacio como campo de batalla

Las operaciones desarrolladas en el ciberespacio, como las acciones criminales o la ciberguerra, pasan desapercibidas para la gran mayoría de los usuarios. Sin embargo, con las herramientas adecuadas, se puede visualizar gráficamente los ciberataques en un colorido intercambio a escala global.

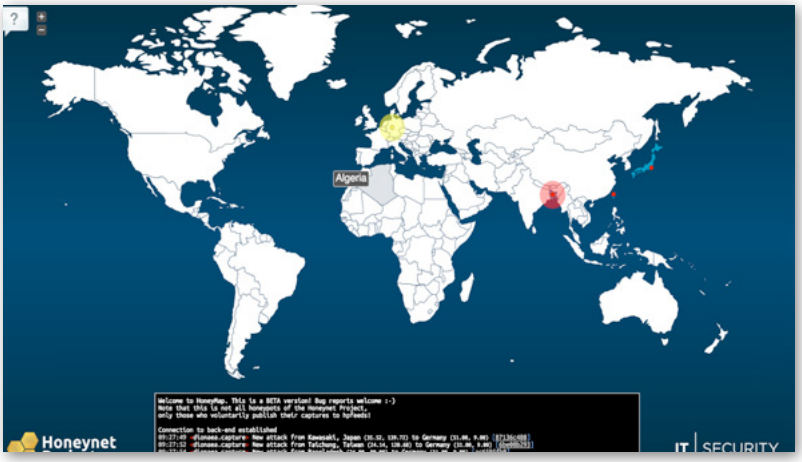
Diversos fabricantes y firmas de seguridad elaboran y mantienen estos mapas de ciberataques en tiempo real. Si bien la determinación de la autoría es difusa, lo verdaderamente sorprendente es la gran cantidad de ataques existentes ejecutados por los diversos actores. De forma general, cuando no se puede fijar el origen con exactitud, el ataque es asignado a una zona, país o región general.

A continuación se muestra una selección de los mapas más relevantes.

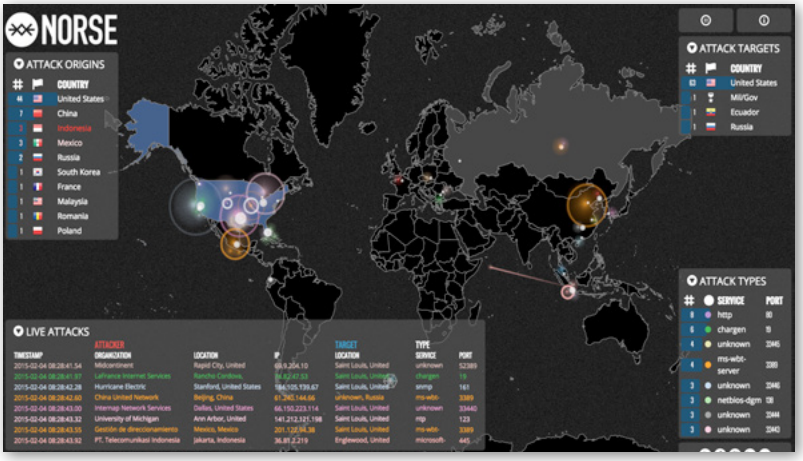
http://www.sicherheitstacho.eu/



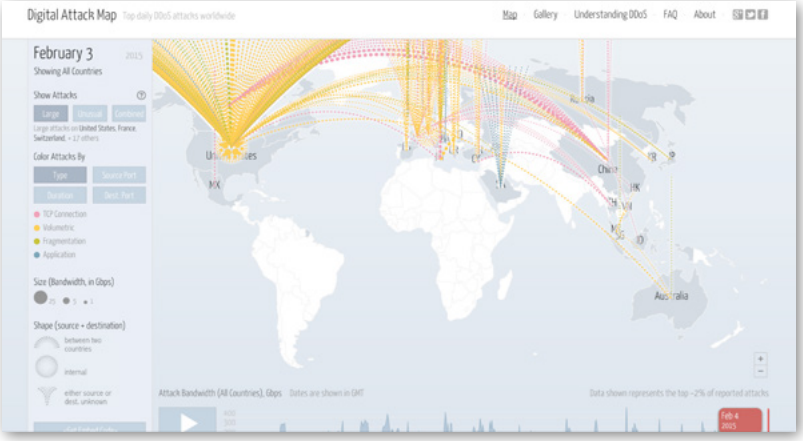
http://map.honeynet.org/



http://map.ipviking.com/



http://www.digitalattackmap.com/



http://cybermap.kaspersky.com/

5 ANÁLISIS DE ACTUALIDAD INTERNACIONAL
La esquizofrénica diplomacia pública de los ayatolás

AUTOR: David Barrancos. Analista internacional. THIBER.

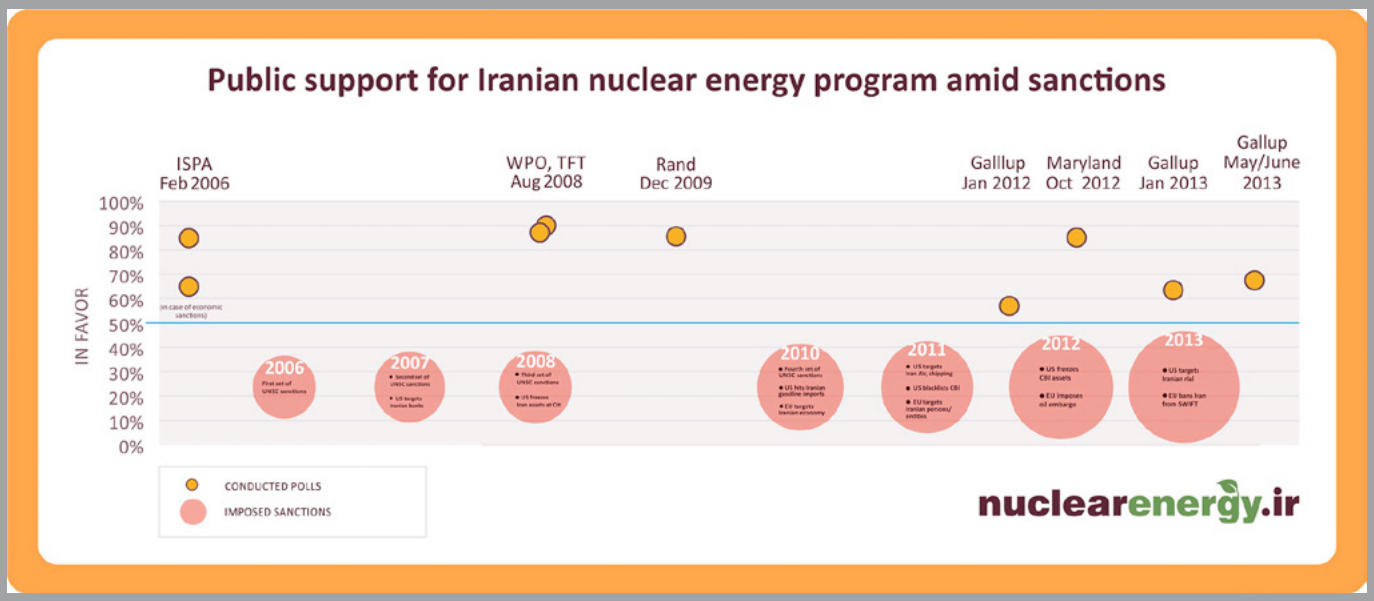
Estocolmo, febrero de 2014. El ministro de Asuntos Exteriores iraní, Javad Zarif, se reúne con su homólogo sueco, Carl Bildt, para dar una rueda de prensa. Cientos de periodistas y fotógrafos se congregan frente a los dos atriles a la espera de las palabras de los mandatarios. Antes de comenzar su discurso, Bildt saca su iPhone y hace una fotografía de la sala abarrotada ante la estupefacta mirada de su compañero iraní. "¿Para qué narices hará una foto ahora?", parecía preguntarse Zarif. Puede que no supiera que Carl Bildt es el ministro tuitero por antonomasia y que acostumbra a compartir todo lo que hace con sus cientos de miles de seguidores. Puede que no acabe de comprender qué es eso de la diplomacia pública digital y para qué sirve. Y puede, también, que no sea del todo consciente de que su país se encuentra inmerso en una ambiciosa, frenética y esquizofrénica campaña de diplomacia pública.

Todo comenzó en septiembre de 2013. El nuevo presidente Hasán Rouhaní había llegado al poder con la intención de cambiar de rumbo la política exterior de su país, lograr que Europa y Estados Unidos levantaran las sanciones y reiniciar con un aire nuevo el proceso de negociaciones sobre la cuestión nuclear. Para alcanzar estas metas había que dejar atrás la actitud de enfrentamiento que había mantenido durante años su antecesor Mahmud Ahmadineyad, y había que cambiar la política de comunicación. En otras palabras, había que trabajar en un acercamiento a Occidente y la diplomacia pública parecía el camino más directo.

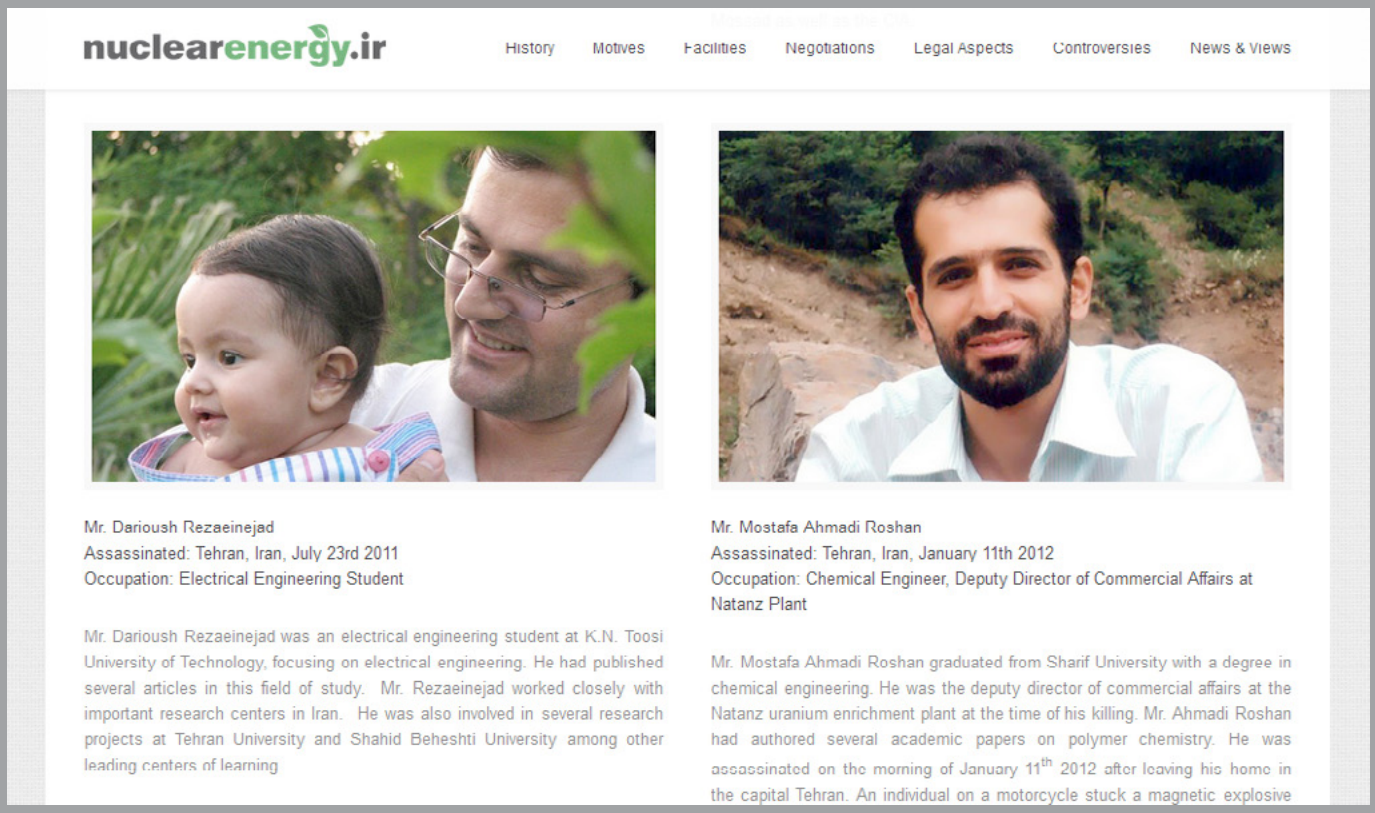
" había que trabajar en un acercamiento a Occidente"

La estrategia comenzó por los medios tradicionales. Rouhaní, por ejemplo, concedió entrevistas a la CNN y a la NBC, y Zarif hizo lo propio con ABC, la revista TIME y el Washington Post. En cuestión de semanas los dirigentes iraníes aparecieron en decenas de medios estadounidenses intentando mostrar la cara más amable de Teherán y dando a conocer sus argumentos. Pero la clave de la campaña no residía en periódicos ni televisiones, sino en la diplomacia digital. En primer lugar se replantearon las páginas web de medios oficiales o semioficiales de Irán como Fars News Agency o Mehr News Agency. Estos sitios web, prácticamente abandonados y con diseños más propios de 1999 que de 2014, apenas traducían sus informaciones al inglés, y en los casos en los que lo hacían se trataba de información obsoleta. Con la nueva campaña se remodelaron todas las páginas web, y ahora ofrecen contenido instantáneo, mucho más visual, y en varios idiomas, desde el inglés y el alemán al turco o el urdu. Si querían comunicar algo tenía que ser atractivo, relevante y en el idioma de sus destinatarios.

En segundo lugar se crearon nuevas plataformas para explicar algunos de los asuntos más controvertidos de la política iraní, como la energía nuclear. Fue así como surgió nuclearenergy.ir, una de las páginas web iraníes más sofisticadas hasta la fecha. En ella se narra la historia del programa nuclear y se explica que su motivación no es militar, sino energética, ecológica e incluso medicinal. Asimismo, en la página se muestran los resultados de diferentes encuestas que prueban que la voluntad del pueblo iraní de desarrollar su programa nuclear no ha disminuido sensiblemente a pesar de las sanciones, y que el gobierno cuenta con su respaldo a la hora de las negociaciones.



Además, la página web reconoce como en pocas veces ha hecho el gobierno iraní que los servicios de inteligencia de Estados Unidos e Israel han logrado introducir virus informáticos en sus centrales nucleares para detener la producción, y que algunos de sus científicos más reconocidos han sido asesinados por su participación en el desarrollo del programa nuclear. La web recoge los perfiles biográficos de estos ingenieros en una sección "In memoriam", en la que se describen crudamente los asesinatos y se pretende demostrar que son otros países y no los iraníes los que siguen políticas agresivas.



En tercer y último lugar, los mandatarios iraníes abrieron cuentas personales en las principales redes sociales algo verdaderamente paradójico en un país en el que Facebook y Twitter no sólo están bloqueados, sino que han sido tachados de pecaminosos por algunos líderes religiosos. Así, tanto Rouhaní como Zarif, emplearon las redes sociales para acercar posturas con sus negociadores occidentales y poner de manifiesto el viraje de la política iraní.

Rouhaní aprovechó su cuenta de Twitter para mostrar sus encuentros junto a los líderes mundiales con los que Ahmadinejad no mantenía ninguna relación. Tras 35 años en los que no se producía una reunión semejante, Rouhaní mantuvo una conversación con el primer ministro David Cameron, e incluso hizo una llamada telefónica al presidente Barack Obama. En apenas unos meses, el "Gran Satán" como se conoce a Estados Unidos en Teherán y sus aliados habían pasado de ser unos asesinos a unos socios con los que mantener un "diálogo constructivo". En la misma línea de ruptura con el conservadurismo anterior, el presidente también mostró en numerosas ocasiones su apoyo a los derechos de las mujeres, y llegó a tuitear una fotografía sin velo de una reconocida matemática iraní, algo que le ha acarreado numerosas críticas entre los sectores menos progresistas de su país.

Sin embargo, lo que realmente superó las líneas rojas de la ortodoxia iraní fue un tuit con el que Zarif estrenó su cuenta en la red social. En ese mensaje el ministro felicitaba a sus seguidores el Rosh Hashaná el año nuevo judío, una provocación en toda regla para un país que desde hace décadas considera al "Pequeño Satán" es decir, a Israel como su enemigo directo.

Parecía evidente que algo estaba cambiando en Teherán. La llegada de Rouhaní había revolucionado la comunicación y la diplomacia de la República Islámica, y un acercamiento con Washington se contemplaba como una posibilidad factible. Pero antes de echar las campanas al vuelo, había que tener en cuenta a un personaje clave, el Líder Supremo y jefe del Estado, Alí Jamenei.

El ayatolá Jamanei también se sumó a la campaña en redes sociales, y desde entonces ha sido uno de los dirigentes iraníes más activos. Sin embargo, su visión sobre la política internacional es diametralmente opuesta a la que Rouhaní intentaba defender, y eso es algo que no ha dudado en compartir con sus seguidores para desgracia de la nueva diplomacia iraní. Así, mientras su primer ministro se reunía con Cameron, Jamenei aseguraba que el grupo terrorista ISIS ha sido creado por el "malvado gobierno británico, que es un especialista en sembrar la discordia entre los musulmanes, para luchar contra Irán". Al tiempo que Rouhaní pretendía conversar con Obama, Jamenei declaraba que los terroristas y los soldados estadounidenses "tienen los mismos objetivos" y que "Estados Unidos tiene las manos manchadas de sangre". Ni siquiera el pueblo estadounidense queda libre de las críticas del ayatolá, quien lo considera "un pueblo profano y sin dios, que amenaza a la humanidad". Pero el asunto donde más serias eran sus diferencias era la relación con Israel. Lejos de felicitar a los judíos como hiciera Zarif, Jamenei prefería avisarles de que si hacían un "movimiento equivocado, Irán arrasará Haifa y Tel Aviv". Y aún más allá, el ayatolá puso en cuestión la existencia del Holocausto, y afirmó que los auténticos genocidas eran los propios israelíes en Palestina.

En la misma línea, Press TV, la cadena de televisión internacional del régimen y uno de los pilares de la propaganda iraní, secundaba sus teorías sobre el Holocausto, afirmaba que la CIA se encontraba detrás del Estado Islámico y hablaba de la OTAN como un club de asesinos. Si su objetivo era evitar el acercamiento, estaban haciendo todo lo posible por conseguirlo.

Aunque podría pensarse que esta falta de coherencia responde a un intento de acallar las críticas internas de los sectores opuestos a la apertura de Rouhaní, lo cierto es que los destinatarios objetivo de los mensajes de Jamanei no son los iraníes, pues estos no han sido escritos en lengua persa y se distribuyen en redes sociales que están prohibidas en Irán. Las diferencias en las redes sociales son, simple y llanamente, un reflejo de los diferentes enfoques políticos entre el Líder Supremo y el Presidente. Esto no quiere decir que Jamenei se muestre en contra de la campaña online de Rouhaní —pues sin su aprobación nunca habría sido posible—, pero sí que es probable que el Presidente esté yendo más lejos de lo que el ayatolá esperaba.

" la nueva política de acercamiento de la República Islámica ya está dando sus frutos"

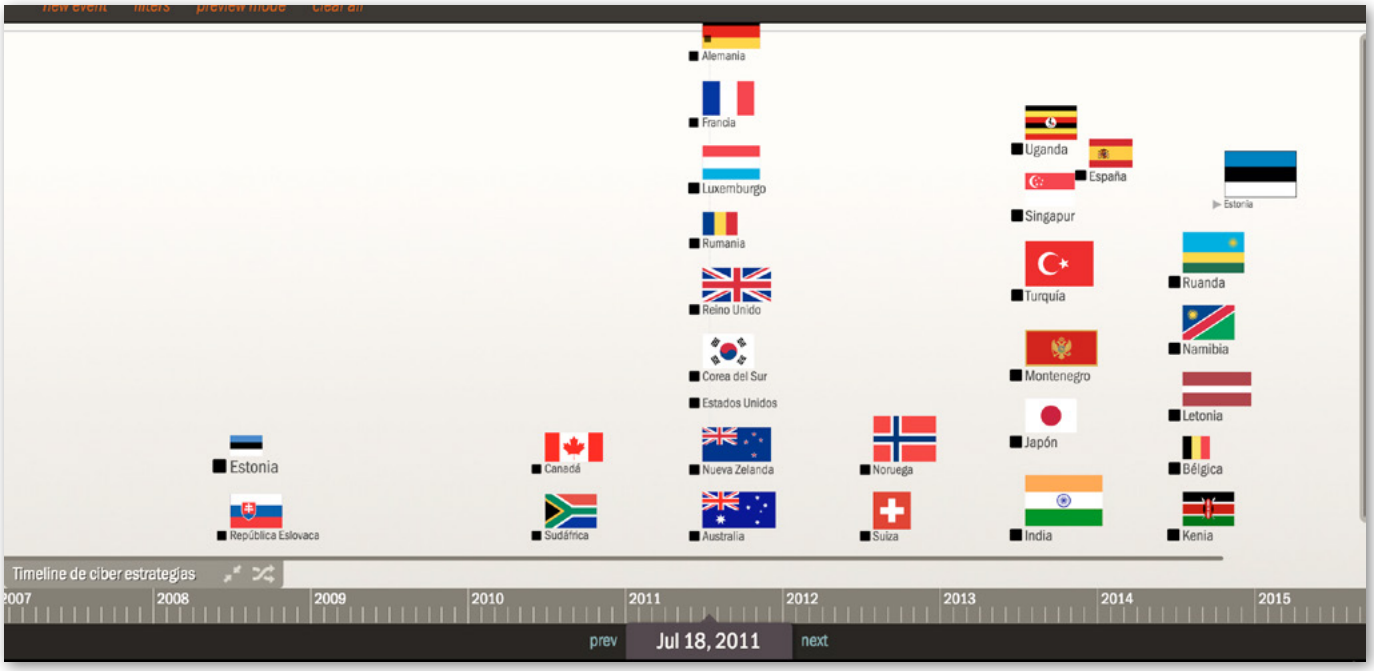
A pesar de todo, según una reciente encuesta de Gallup el porcentaje de estadounidenses que ven a Irán como el primer enemigo de su país se ha reducido a la mitad desde la llegada de Rouhaní. Además, el porcentaje de personas que tiene una opinión muy negativa del país ha disminuido considerablemente, y ha aumentado el de personas que tienen una opinión positiva. La conclusión, por tanto, es que la nueva política de acercamiento de la República Islámica ya está dando sus frutos y la imagen del país está cambiando. Sin embargo, es igualmente cierto que estos esfuerzos sufren un torpedeo diario por parte de personajes como Jamenei, que no acaban de comprender que la imagen del país en el exterior no admite diferencias ideológicas ni divisiones institucionales. Para los ciudadanos occidentales Irán es un todo, y por eso resulta tan confuso que el mismo país que un día te felicita el año nuevo te amenace al día siguiente con bombardear tu ciudad, que el mismo país que charla amigablemente con tu presidente te ataque al día siguiente y te tache de asesino. Sólo cuando la diplomacia pública iraní sea una política coherente y uniforme logrará tener un efecto a largo plazo y resultados sólidos. Hasta entonces, Occidente seguirá pensando que habla con un país esquizofrénico.

6 Estrategias nacionales de ciberseguridad en el mundo

Bajo estas líneas se muestra una recopilación de las principales estrategias de ciberseguridad nacionales y supranacionales actualizadas.

Adicionalmente se ha creado un timeline gráfico reflejando su fecha de publicación inicial, desde el año 2000.

http://timeglider.com/timeline/0043b0040a9001cb



7 Entrevista a Joaquín Castellón.

Director Operativo del Departamento de Seguridad Nacional.

1. Como Director Operativo del Departamento de Seguridad Nacional, usted ha sido artífice, en buena media, y testigo privilegiado de la puesta en pie en España del Sistema de Ciberseguridad Nacional. ¿Podría trazar sus grandes hitos y destacar sus elementos más novedosos?

Creo que es justo situar el comienzo de este proceso en julio de 2012, mes en que se crea el Departamento de Seguridad Nacional, en el seno del Gabinete de la Presidencia del Gobierno. El Departamento nace con la idea de impulsar una nueva concepción de la Seguridad Nacional, acometiendo inicialmente la tarea de revisar la Estrategia Española de Seguridad de 2011 del anterior Ejecutivo, un texto elaborado bajo la dirección de Javier Solana. Fruto de casi un año de trabajo, a finales de mayo, el Consejo de Ministros aprobaba la Estrategia de Seguridad Nacional de 2013.

Quiero destacar que por primera vez nos dotamos en España de forma simultánea de la combinación de un documento estratégico del más alto nivel y su desarrollo orgánico inmediato, el Consejo de Seguridad Nacional. En este sentido, la Estrategia es un documento orientado a la acción. En este documento, se responde a una visión integral de la Seguridad y se presentan doce riesgos y amenazas con un enfoque innovador y transversal. Ámbitos tales como la ciberseguridad conviven con otros más tradicionales como la defensa nacional o la lucha contra el terrorismo.

El elemento orgánico principal del Sistema es el Consejo de Seguridad Nacional, que se reúne a iniciativa del Presidente del Gobierno y reúne a las figuras más relevantes con competencia en materia de Seguridad Nacional, si bien su composición es flexible, abierta y modular: autoridades de la administración del Estado; de las Comunidades Autónomas o del sector privado. Las reuniones son presididas por el Presidente del Gobierno, salvo cuando S.M. el Rey asiste a las reuniones, circunstancia que se ha producido en dos ocasiones.

El Consejo aprobó, en diciembre de 2013, la Estrategia de Ciberseguridad Nacional. Como la Estrategia de Seguridad Nacional, la Estrategia de Ciberseguridad Nacional fue coordinada por el Departamento de Seguridad Nacional y su resultado es tan importante como el proceso de elaboración, que estuvo participado por todos los actores clave en la materia y dejó en el histórico la convicción basada en la experiencia de que la ciberseguridad es cooperativa, nacional e internacionalmente.La Estrategia establece los componentes esenciales del Sistema de Ciberseguridad Nacional, que básicamente son:

- El Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional.
- El Consejo Nacional de Ciberseguridad, como órgano colegiado de apoyo al Consejo de Seguridad Nacional, cuya función principal es el fomento de la coordinación, cooperación y colaboración entre Administraciones Públicas y entre éstas y el sector privado. Se encuentran representados todos los ministerios con competencias en materia de ciberseguridad.
- Y por último el Comité de Situación, que apoyándose en el Centro de Situación del Departamento de Seguridad Nacional, presta apoyo al Consejo de Seguridad Nacional en la dirección político-estratégica de situaciones de interés para la Seguridad Nacional, es decir, aquellas que por su transversalidad o su dimensión desborden las capacidades de respuesta de los mecanismos habituales.

2. Según nos comenta ha sido mucho lo avanzado en España en ciberseguridad nacional y esto es claramente así desde el punto de vista de los órganos que se han creado para reforzar la visión integral de la ciberseguridad. ¿Qué éxitos se están logrando desde un punto sustantivo? ¿Es esta orgánica útil? ¿Nos haría falta algo más?

Creo sinceramente que en este último año se ha avanzado mucho en todo lo relativo a la ciberseguridad en España y en buena medida estos avances parten y se explican por la Estrategia de Ciberseguridad y la puesta en marcha del Consejo de Ciberseguridad Nacional. Entre los logros, me gustaría destacar la aprobación, el 31 de octubre de 2014 por el Consejo de Seguridad Nacional, del Plan Nacional de Ciberseguridad. Este plan asigna cometidos a los órganos y organismos representados en el Consejo de Ciberseguridad Nacional. Un plan es un camino y un propósito. Su aprobación es en sí positiva. Pero no podemos quedarnos ahí.

Si bien se está avanzando de manera notoria en un ámbito que presenta grandes retos para las sociedades y los gobiernos a nivel global, existen ciertas lagunas y temas complejos no resueltos que aún nos quedan por abordar. De esto somos muy conscientes en el Departamento de Seguridad Nacional. Se requiere un esfuerzo de adaptación y en algunos casos de cambio en nuestra forma de organizarnos y nuestro modo de trabajar.

Desde el Departamento estamos impulsando, por citar un par de ejemplos, la puesta en marcha o el perfeccionamiento de mecanismos e instrumentos que faciliten la coordinación, cooperación y el intercambio de información entre los diferentes organismos estatales, y en este mismo sentido, creemos también primordial desarrollar mecanismos y herramientas que faciliten el intercambio de información sobre ciberamenazas y ciberincidentes entre los sectores público y privado.

3. Una de las críticas ante la Estrategia era que no parecía existir una atribución presupuestaria directa, ¿cree que esto es un problema?

Digamos que hay dos formas de ejecutar un Plan: que nazca con un presupuesto previo o que se elabore y se estudie en primer lugar, se identifiquen los proyectos, se cuantifiquen económicamente y se prioricen para su ejecución. En nuestro caso hemos optado por esta segunda opción que creemos es lo más razonable.

A ello hay que añadir la creación o refuerzo de nuevos o ya existentes organismos con competencias en este ámbito, como el Mando Conjunto de Ciberdefensa o el recientemente creado CERT de Defensa, la Oficina de Coordinación Cibernética del CNPIC, el CERT de Seguridad e Industria, o la Dirección General TIC de la Administración General del Estado (AGE), lo que unido a los presupuestos de los organismos ya existentes comprenden un montante presupuestario nada desdeñable.

4. Recientemente se hacía público por parte de la Administración el dato de que España es el tercer país con mayor número de ciberataques tras EEUU y Reino Unido. ¿Cómo se explica esta cifra? ¿Cómo debe interpretarla el ciudadano?

Este tipo de rankings aunque útiles, como orientación general, tienen solo el valor que tienen, dependiendo de los criterios elegidos puede salir un resultado u otro. Lo que es irrefutable es que en países como EEUU, Reino Unido, Francia, Alemania, Italia o España el número de ciberincidentes está aumentando de forma exponencial y constituye una prioridad absoluta en la agenda de seguridad de los diferentes Gobiernos.

" el número de ciberincidentes está aumentando de forma exponencial"

Todos los países estamos haciendo un gran esfuerzo por reforzar nuestras capacidades de prevención, detección, coordinación y respuesta ante las ciberamenazas y podemos sentirnos tan seguros o inseguros como el resto de países de nuestro entorno.

En referencia a los países que menciona en su pregunta, es público y notorio el gran esfuerzo que están haciendo por mejorar sus capacidades ante los ciberataques, como lo han manifestado recientemente en público el Presidente de los Estados Unidos y el Primer Ministro británico. Ambos países han puesto en marcha nuevos organismos encaminados a garantizar una mayor coordinación y cooperación entre los diferentes actores de la ciberseguridad. En el caso de Reino Unido esta idea se concretó con la constitución del CERT UK y en el caso norteamericano se ha anunciado recientemente la creación del Centro de Integración de Inteligencia Contra las Ciberamenazas. Estos dos ejemplos son una referencia válida para mejorar la coordinación y el intercambio de información entre los equipos de respuesta a incidentes en ciberseguridad nacionales.

En España, en la actualidad se está impulsando de forma innovadora la gestión de crisis de cualquier naturaleza en el nivel político-estratégico y es precisamente en este punto donde también se debe reforzar la acción en materia de ciberseguridad, de forma que los niveles operativo, táctico y político-estratégico estén perfectamente sincronizados, y, así, ante crisis mayores se asegure el uso óptimo de los recursos y se ofrezcan respuestas eficaces, prontas y completas.

5. A la vista los acontecimientos recientes (como el uso del ciberespacio por parte del Estado Islámico), ¿cree que el ciberespacio sirve para ejercer poder? ¿Cómo?

Se calcula que actualmente cerca de tres mil millones de personas estamos conectados en la red y que, tan solo en diez años, la cifra podría rondar los siete mil millones de personas. Creo que es un dato bastante elocuente de las posibilidades del ciberespacio para ejercer poder.

En el caso concreto de las organizaciones terroristas, hace escasas semanas el Gobierno aprobó el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta, Plan que pretende prevenir y evitar el surgimiento y desarrollo de procesos de radicalización violenta y su posible evolución hacia el terrorismo. El Plan establece tres ámbitos de actuación: el interno, el externo y el ciberespacio. La importancia que otorga el Plan al ciberespacio es una consecuencia directa del uso creciente del mismo por parte de grupos terroristas, fundamentalmente en actividades orientadas a la captación y financiación.

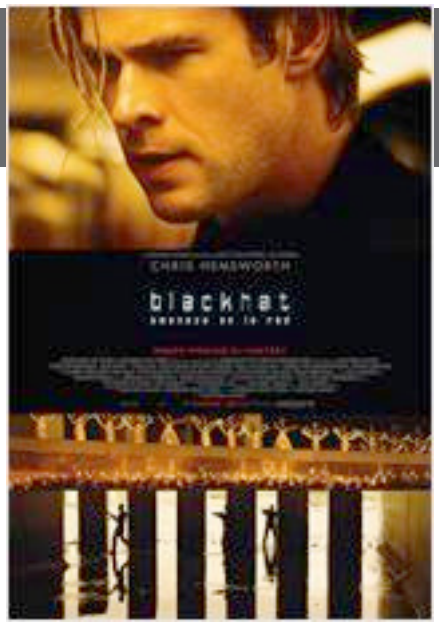
6. Tal y como plantea la Estrategia de Seguridad Nacional, el ciberespacio es un nuevo dominio. ¿Cree que todos los actores, tanto públicos como privados, han observado la importancia de este dominio?

En este caso permítaseme la expresión "la necesidad obliga", las cifras de fraude, espionaje industrial, etc… hablan por sí solas. Lamentablemente en general podemos decir que se ha reaccionado tarde y esto conlleva un esfuerzo adicional por parte de todos, sector público, privado y de la sociedad en general. El ciberespacio es un entorno que ha crecido muy rápido en muy pocos años, lo que ha supuesto un auténtico desafío para los Estados a la hora de adaptar al mismo ritmo sus estructuras y legislaciones. También implica un cambio de mentalidad grande en las empresas y en nuestra vida diaria como ciudadanos de a pie.

Consciente de ello, en España con los documentos y estructuras creadas se han marcado las directrices sobre las que establecer la protección del ciberespacio para que todos los españoles puedan hacer un uso libre y seguro de él, pero para ello es necesario crear una fuerte cultura de ciberseguridad que impacte a la sociedad en su conjunto y a todos los niveles.

8 Recomendaciones

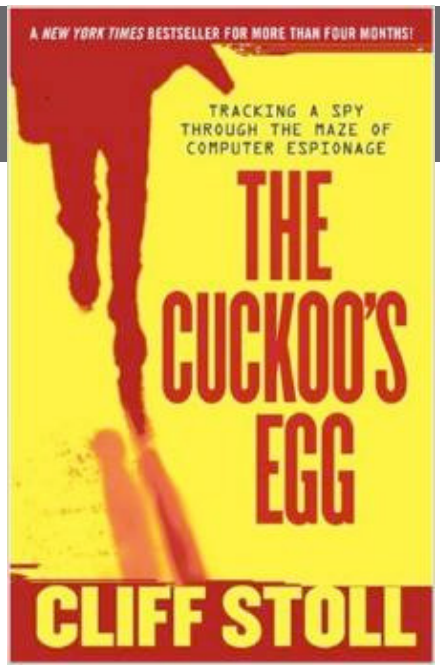
8.1 Libros y películas



Película:
BLACKHAT

Sinopsis: Los gobiernos estadounidense y chino se ven obligados a cooperar por el bien de la seguridad nacional de ambas potencias. Una fuerte amenaza informática está poniendo en riesgo las vidas y el futuro de la población. Delitos informáticos de alto nivel para los que deberán recurrir a sus mejores agentes de campo si quieren llegar a tiempo para evitar lo peor.

Acción y suspense son los ingredientes de esta película protagonizada por Chris Hemsworth, Spencer Garrett y Viola Davis, entre otros, bajo la dirección de Michael Mann.

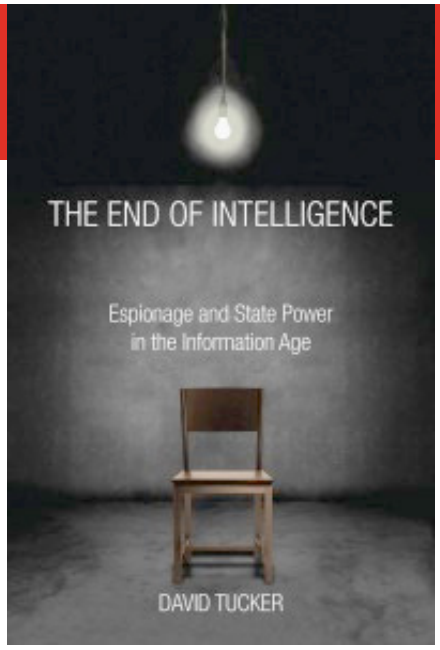


Libro:
THE CUCKOO'S EGG

Autor: Cliff Stoll
Num. Páginas: 399
Editorial: Pocket Books
Año: 1989
Precio: 9,50 Euros
Sinopsis: Basado en hechos reales, un error de contabilidad de 75 centavos destapa una interesante historia de ciberespionaje en el que se verán involucrados los principales servicios secretos estadounidenses y europeos.

Libro:
@WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX

Autor: Shane Harris
Num. Páginas: 288
Editorial: Eamon Dolan
Año: 2014
Precio: 15,00 Euros
Sinopsis: Apasionante relato de la evolución de la ciberguerra durante la ultima década, prestando especial atención a la evolución de la Agencia Nacional de Seguridad (NSA) y el U.S Cyber Command. Shane Harris aborda los principales debates que tienen al ciberespacio como protagonista: Atribucion, ciber-retorsion y la guerra criptográfica.



Libro:
THE END OF INTELLIGENCE

Autor: David Tucker
Editorial: Stanford University Press
Año: 2014
Precio: 19,50 Euros

Sinopsis: Usando el espionaje y el ciberespionaje como un caso de análisis, “El Fin de la Inteligencia” de David Tucker critica las afirmaciones de que la reciente revolución de la información ha debilitado al Estado, revolucionado la guerra, y cambiado el equilibrio de poder entre los Estados y actores no estatales.

El examen de espionaje, contraespionaje, y acciones encubiertas, el libro sostiene que, contrariamente a las opiniones imperantes, la revolución de la información y el ciberespacio están aumentando el poder de los Estados en relación con los actores no estatales, afectando a la privacidad. Argumentando que los organismos de inteligencia puede ser tomadas como las organizaciones paradigmáticas de la era de la información, el autor David Tucker muestra los límites de la recolección y análisis de información, incluso en estas organizaciones.

Este libro desafiará lo que creemos saber sobre el poder de la información y el Estado, y sobre el potencial destino de la privacidad y el secreto en el S. XXI

8.2 Webs recomendadas

Bitácora de Kaspersky labs mostrando algunas de las ciberamanezas persistentes avanzadas (APT) más sofisticadas
https://apt.securelist.com/#firstPage

El Centro Criptologico Nacional, creado en el año 2004, a través del Real Decreto 421/2004 y adscrito al Centro Nacional de Inteligencia (CNI), es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.
www.ccn.cni.es

THIBER es el primer think tank nacional en material de ciberseguridad y ciberdefensa
www.thiber.org

SDB es un referente nacional íntegramente dedicado a la ciberseguridad en su vertiente técnica.

www.securitybydefault.com

El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo público cuyo objetivo es desarrollar la Sociedad de la Información mediante la innovación y el desarrollo de proyectos relacionados con la cibserseguridad nacional e internacional.

www.incibe.es

8.3 Cuentas de Twitter

@schneierblog

@USCERT_gov

@info_CCI

@INCIBE

@THIBER_ESP

9 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1-6 de marzo	Valencia	Circumvention Tech Festival	Circumvention Tech Festival	www.circumventionfestival.es
2,3,4 marzo	Madrid	RootedCON	RootedLabs	www.rootedcon.com/rootedlabs
5,6,7 marzo	Madrid	RootedCON	RootedCON 2015	www.rootedcon.com
10, 11 y 12 de marzo	Madrid	Grupo Atenea	HOMSEC 2015	www.homsec.es
16-20 de marzo	Hannover	CeBIT	CeBIT 2015	www.cebit.de
9-13 marzo	Miami	Microsoft	Digital Crimes Consortium 2015	www.microsoft.com
10 marzo	Buenos Aires	Segurinfo	Segurinfo 2015	www.segurinfo.org
18-20 marzo	Corea		SECON 2015	www.seconexpo.com
26 marzo	Paraguay	Segurinfo	Segurinfo 2015	www.segurinfo.org
26 marzo	Madrid	OWASP	I Evento OWASP Madrid	www.ticketea.com/i-evento-owasp-madrid
29, 30 y 31 de Marzo	Frankfurt	Asis International	ASIS 14th European Security Conference & Exhibition	www.asisonline.org/Education-Events/Global-Conferences/2015-European-Security-Conference-and-Exhibition/Pages/default.aspx

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