REAL INSTITUTO elcano ROYAL INSTITUTE

ENERO 2018
Nº 32

CIBERelcano

Informe mensual de ciberseguridad

Desarrollado por: THIBER

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.

Informe editado en Madrid.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 Análisis de actualidad internacional 04

2 Ciberpolítica: análisis de actualidad 10

3 Informes y análisis sobre ciberseguridad publicados en diciembre 13

4 Herramientas del analista 14

5 Análisis de los ciberataques del mes de diciembre 15

6 Recomendaciones

6.1 Libros y películas 21

6.2 Webs recomendadas 23

6.3 Cuentas de Twitter 23

7 Eventos 24

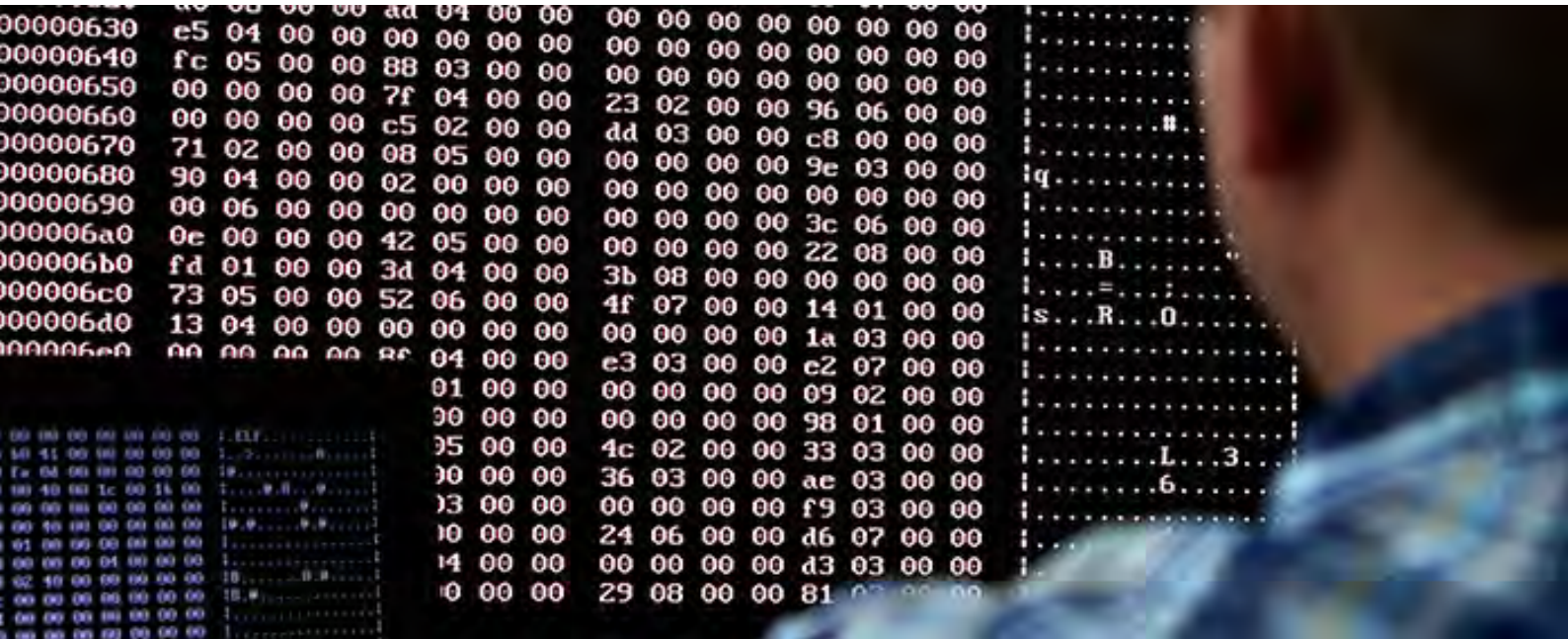
1 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Contextualizando la guerra híbrida

AUTORES: Guillem Colom, Director de THIBER, the cybersecurity think tank.

El concepto de guerra híbrida se ha convertido – junto con las noticias falsas, los trolls, los bots o la desinformación – en uno de los *hype* informativos del 2017 a pesar de las controversias que genera. Muchos expertos consideran que no existen razones objetivas para acuñar nuevas denominaciones que sólo añaden confusión al análisis estratégico. Otros sostienen que el conflicto híbrido es el resultado natural de la adaptación de la guerra irregular al mundo actual. Otros subrayan que este concepto no está consolidado ni existe ninguna definición aceptada por la comunidad de defensa más allá del mínimo común denominador de la combinación de medios, procedimientos y tácticas convencionales y asimétricas. Finalmente, muchos alertan de que esta idea corre el riesgo de perder su valor explicativo al haberse popularizado para definir cualquier actividad realizada por un estado o actor no-estatal sin cruzar la frontera entre paz y guerra, poniendo como ejemplos casos tan dispares como las intervenciones rusas en Crimea o Ucrania, sus acciones de desestabilización en su área de influencia directa o las operaciones informativas alrededor del globo. Teniendo estos elementos en cuenta, el artículo expondrá brevemente los orígenes, concepción y debates actuales sobre el concepto de guerra híbrida.

Definido originalmente en un trabajo académico de la Armada estadounidense de 2002 para advertir de las tácticas empleadas por la insurgencia chechena contra el ejército ruso, el término guerra híbrida fue empleado por primera vez en la *Estrategia de Defensa Nacional* norteamericana tres años después para explicar la combinación de dos o más amenazas de tipo tradicional, irregular, catastrófico o disruptivo. Sin embargo, no fue hasta la publicación del artículo *La guerra del futuro: la llegada del conflicto híbrido*, escrito por el titular del Pen-



tágono James N. Mattis junto con el teniente coronel Frank G. Hoffman cuando se le dotó de contenido teórico, la guerra de 2006 entre Israel y Hezbollah cuando pareció tener lugar su primera gran manifestación práctica, y la presentación del ensayo *El conflicto en el siglo XXI*: *el advenimiento de la guerra híbrida* cuando se popularizó. Sin embargo, no sería hasta varios años después cuando, a raíz de las reflexiones del jefe de estado mayor de la defensa rusa Valeri Gerasimov, las intervenciones de Moscú en Crimea y Ucrania o sus operaciones de información en varios países occidentales, la guerra híbrida traspasó la frontera del debate estratégico para convertirse en un vocablo de uso común. Sin embargo, al asimilar la guerra híbrida con las acciones rusas obviando su larga experiencia en materia de propaganda y agitación, este concepto corre el riesgo de perder su valor explicativo y convertirse en una idea vacía de contenido o un sinónimo de las acciones rusas en la "zona gris".

"Tras las intervenciones de Moscú en Crimea y Ucrania o sus operaciones de información en varios países occidentales, la guerra híbrida traspasó la frontera del debate estratégico para convertirse en un vocablo de uso común"

A pesar de haberse popularizado para definir una tipología de conflicto que combina el empleo de medios regulares e irregulares o explicar las aparentemente novedosas tácticas de Moscú, la guerra híbrida no es el único concepto barajado actualmente para explicar la transformación de los conflictos. Al contrario, junto con la popularización del concepto de "zona gris" para referirse a cualquier actividad militar o no-militar ejercida con más o menos ambigüedad en la amplia franja que existe entre la paz y la guerra abierta pero sin entrañar un *casus belli*, la amenaza híbrida es la más reciente y sugestiva de una larga serie de expresiones – conflictos de cuarta y quinta generación, de tres bloques, posmodernos, compuestos, entre la población, complejo-irregulares o sin restricciones – concebidas desde el fin de la Guerra Fría para definir las "nuevas guerras" del siglo XXI.

Estos conflictos calificados como característicos del mundo globalizado son presentados como novedosos tanto por los actores involucrados (estados interviniendo de manera directa o delegando su actuación a agentes domésticos, guerrillas, terroristas, redes criminales o contratistas militares privados), los medios utilizados (armas sencillas empleadas de manera novedosa, sistemas sofisticados a disposición de los estados, armas pesadas o tecnologías de uso dual disponibles en el mercado), las tácticas empleadas (acciones convencionales limitadas, actos terroristas, insurgencia, ciberoperaciones, ocultación y engaño o propaganda multicanal), los multiplicadores usados (sistemas de posicionamiento, inteligencia de fuentes abiertas (OSINT) y de redes sociales (SOCMINT), *drones*, comunicaciones avanzadas o ciberataques) o las fuentes de financiación manejadas (actividades legales y delictivas con estrecha colaboración con el crimen organizado).

Estas características hacen que las “nuevas guerras” del siglo XXI sean aparentemente muy distintas de los conflictos más representativos – pero en absoluto los únicos – de la Era Moderna o Contemporánea, donde existía una declaración formal de guerra que impedía el surgimiento de “zonas grises” y donde los ejércitos regulares pertenecientes a un estado-nación combatían convencional y simétricamente en frentes definidos, respetando los usos y costumbres de la guerra y utilizando medios tecnológicamente avanzados para la época. Por lo tanto, no es extraño imaginar que cualquier adversario, cuando se enfrente a un ejército occidental, intentará aprovechar las oportunidades que le brinda el mundo globalizado para explotar las limitaciones del estilo occidentalizado de combatir, fundamentado éste en la supremacía tecnológico-militar y en el cumplimiento de las leyes y costumbres de la guerra para lograr victorias rápidas, decisivas, contundentes y sin apenas bajas propias ni daños colaterales. En consecuencia, tal y como ha sucedido desde la antigüedad clásica, ante la imposibilidad de medirse con un ejército avanzado, el enemigo utiliza tácticas asimétricas, se confunde entre la población, actúa ajeno a los usos y costumbres de la guerra e intenta que sus actividades tengan los mayores efectos estratégicos posibles mediante una eficaz explotación informativa de sus actos.

Ante un escenario marcado por la supremacía militar de los ejércitos regulares avanzados, cualquier oponente – desde los paramilitares albano-kosovares contra Serbia y ésta contra la Alianza Atlántica, las guerrillas chechenas contra Rusia, las milicias de Hamas y Hezbollah contra Israel, la insurgencia talibán, la resistencia iraquí o Daesh contra sus enemigos y hasta Rusia, conocedora de su inferioridad militar convencional sobre la Alianza Atlántica – se ve obligado a adaptarse y plantear respuestas que mitiguen esta superioridad y exploten las debilidades políticas, sociales, jurídicas, morales, económicas, demográficas o militares de estos adversarios aparentemente imbatibles en el terreno convencional.

Mientras cualquier oponente estatal o no-estatal parece hacer gala de un realismo extremo y sabe aprovechar sus fortalezas y minimizar sus debilidades, las sociedades occidentales han abrazado los valores posmodernos y posmaterialistas. Éstos impiden ver el mundo como algo complejo y peligroso, donde el poder, el interés y la ambición pueden provocar choques violentos y donde las controversias internacionales pueden resolverse pacíficamente con arreglo al derecho internacional. Es por esta razón que nuestras sociedades – especialmente las europeas occidentales – son cada vez más reacias a concebir el empleo de la fuerza o la amenaza de recurrir a ella como herramienta de política exterior para defender los intereses o la soberanía nacional. En este contexto, nuestro poder militar se convierte en irrelevante y nuestra capacidad disuasoria en inverosímil si carecemos de la voluntad de utilizar la fuerza o advertir de forma creíble que cualquier alteración del *status quo* podrá motivar una respuesta clara y contundente. Junto con la desafección política y la explotación del juego democrático, esta falta de credibilidad de la disuasión está motivando la escalada en el número e intensidad de las actividades en esta "zona gris" que separa la paz de la guerra o la proliferación de las operaciones de información en el ciberespacio sin que occidente pueda plantear ninguna réplica efectiva.

"Considerada como una el estilo de lucha característico de la Era de la Información que se distingue por la combinación, en todos los niveles y fases de la operación, de acciones convencionales e irregulares, mezcladas éstas últimas con actos terroristas, propaganda y conexiones con el crimen organizado."

En el marco de las operaciones militares, la situación tampoco es mejor. La volubilidad de la opinión pública doméstica y la presión de la comunidad internacional, el pánico a las bajas propias y el temor a los daños colaterales, el sometimiento a unos usos y costumbres de la guerra restrictivos y anacrónicos, la ansiedad por los costes políticos y los efectos electorales de las operaciones, la exigencia de restringir su alcance, impacto y duración, la renuencia a usar fuerzas terrestres en operaciones o la necesidad de emplear la fuerza de manera limitada y restrictiva son otros elementos que pueden ser explotados por los actores estatales y no-estatales que se enfrentan contra un ejército occidental. La unión de todos estos factores sienta las bases para la construcción del concepto de guerra híbrida.

Considerada como una el estilo de lucha característico de la Era de la Información que, fundamentado en las posibilidades que brinda la globalización y el libre acceso a las tecnologías avanzadas, se distingue por la combinación, en todos los niveles y fases de la operación, de acciones convencionales e irregulares, mezcladas éstas últimas con actos terroristas, propaganda y conexiones con el crimen organizado. De forma más específica, según Frank G. Hoffman, el creador del concepto, la guerra híbrida consiste en: *"…una amenaza que, susceptible de ser utilizada tanto por estados como por actores no-estatales,*

aprovecha toda la gama de modos y estilos de lucha disponibles. Éstos pueden incluir formas convencionales; tácticas y orgánicas irregulares, actos terroristas fundamentados en el uso de la violencia y la coerción de forma indiscriminada; e incluso actos criminales."

En consecuencia, la guerra híbrida se caracteriza por la integración en tiempo y espacio de procedimientos convencionales con tácticas propias de la guerra irregular (desde acciones de propaganda, agitación, subversión, guerra de guerrillas e insurgencia hasta labores de guerra informativa, guerra legal (lawfare) o ciberoperaciones), mezcladas éstas últimas con actos terroristas y conexiones con el crimen organizado para la financiación, obtención de apoyos y asistencia. En consecuencia, tal y como hemos podido observar recientemente en Oriente Medio o en Ucrania, la tipología, el estatuto legal o la organización del combatiente es un factor secundario a la hora de caracterizar la amenaza híbrida, puesto que aquello realmente representativo es su habilidad para emplear de forma simultánea y con eficacia procedimientos convencionales, irregulares y terroristas.

A este rasgo distintivo se le suman otras características que podríamos calificar de secundarias como son:

- El empleo de armamento y material tecnológicamente avanzado procedente tanto de los arsenales militares de un país y operado por un ejército o un actor no-estatal, como obtenido en el mercado civil (drones, armas de precisión, medios de inteligencia, comunicaciones avanzadas o cibercapacidades).

- La eficaz explotación de la propaganda e información online para difundir su mensaje, generar narrativas que apoyen sus fines y erosionar las opiniones públicas de sus oponentes.

- La organización interna flexible, adaptable y articulada en red.

- La indefinición normativa y desprecio a los usos y costumbres de la guerra tradicionalmente aceptados por la comunidad internacional.

- La eficaz combinación de los medios que están a su disposición para infligir el máximo daño físico y psicológico a su adversario.

Tal y como habrá advertido el lector, la guerra híbrida es un concepto novedoso, atractivo y con gran fuerza expresiva por dos grandes razones: muestra gráficamente la creciente complejidad de los conflictos actuales y pone de manifiesto la difuminación de las fronteras entre pre-crisis y guerra, entre fuerzas regulares e irregulares o entre tácticas convencionales y asimétricas. Sin embargo, como teoría es imprecisa y como concepto corre el riesgo de perder su significado hasta convertirse en algo irrelevante, especialmente hoy en día, cuando cualquier actividad que pueda relacionarse con Moscú – desde su intervención militar en Ucrania, el *hackeo* de los correos del Comité Nacional Demócrata estadounidense, los anuncios en *Facebook* durante sus comicios presidenciales o la propaganda online sobre Cataluña – es calificada como constitutiva de una guerra híbrida.

Mientras en base a los argumentos expuestos podríamos considerar que Moscú libró una guerra híbrida en Ucrania (aunque siempre teniendo en cuenta que las referencias rusas al concepto son interpretaciones de los debates

occidentales y las publicitadas reflexiones de los generales Makarov y Gerasimov no constituyen ninguna doctrina sino que enlazan con la tradición operativa soviética/rusa), el resto de sucesos no pueden calificarse como tales por una sencilla razón: no nos hallamos ante un conflicto que entrañe el empleo combinado de medios y tácticas militares regulares e irregulares, que sería la definición mínima de guerra híbrida. Al contrario, estos sucesos – incluyendo las actividades que han tenido lugar en el ciberespacio ucraniano – deberían ser calificados como operaciones de información que, herederas de las tradicionales tácticas de desestabilización y agitación soviéticas, pueden realizarse en tiempo de paz, pre-crisis y guerra en los niveles estratégico, operacional o táctico. Además, si tenemos en cuenta que muchos tratadistas militares rusos sugieren la difuminación de la frontera entre paz y guerra y el surgimiento de una "zona gris" del conflicto, parece más acertado empezar a utilizar los conceptos correctamente para evitar que éstos pierdan su significado.

En resumen, bien sea para definir el empleo simultáneo de medios convencionales e irregulares, para mostrar la complejidad de los conflictos actuales o para alertar sobre la peligrosidad de la guerra irregular y asimétrica del siglo XXI, la guerra híbrida no sólo constituye una respuesta lógica al paradigma estratégico reinante en occidente y una forma efectiva de enfrentarse a un adversario militarmente más poderoso, sino que constituye una importante amenaza a la que deben enfrentarse los ejércitos actuales. Sin embargo, no debemos caer en el error de usar esta idea para cualquier suceso extraño, ni realizar interpretaciones interesadas, ni tampoco obviar la capacidad de muchos actores no-estatales para presentar una oposición híbrida, y empezar a reflexionar seriamente sobre la expansión de las zonas grises, estudiar las operaciones de información y plantear de una vez por todas la extrema necesidad de disponer de medios para la comunicación estratégica.

"la guerra híbrida no sólo constituye una respuesta lógica al paradigma estratégico reinante en occidente y una forma efectiva de enfrentarse a un adversario militarmente más poderoso, sino que constituye una importante amenaza a la que deben enfrentarse los ejércitos actuales."

2 CIBERPOLÍTICA: ANÁLISIS DE ACTUALIDAD

La UE afronta nuevos retos en la ciberseguridad del IoT en 2018

AUTORES: Javier Alonso Lecuit. Miembro Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

La UE afronta nuevos retos en la ciberseguridad del IoT en 2018

El IoT experimenta un crecimiento explosivo (8.4 billones de elementos IoT conectados en 2017 y 20 billones previstos en 2020) debido al papel que adquieren las plataformas IoT en la digitalización del sector de consumo (domótica), los procesos de producción (Industria 4.0) y las infraestructuras públicas *(smartcities).* La adquisición y análisis de grandes volúmenes de datos en tiempo real mediante algoritmos de inteligencia artificial *(Big Data)* dotan de inteligencia autónoma a los servicios y aplicaciones IoT, que son la base para la explotación comercial de los datos *(Data Economy). Las predicciones de Forrester Research para 2018* apuntan a un salto del IoT al ámbito comercial apoyado en la externalización de las plataformas IoT de los centros de datos privados hacia entornos de cloud públicos y en la descentralización y la inteligencia autónoma *(edge computing intelligence networks)* del procesado de los dispositivos IoT.

Por un lado, esta compleja dinámica plantea importantes retos debido a la actual fragmentación de los estándares, a la escala global de las plataformas IoT y a la disparidad de requisitos exigidos por cada sector de aplicación. También establece nuevos retos legales y regulatorios vinculados a la protección de la privacidad, los derechos de propiedad de la información, la transferencia internacional de datos o la responsabilidad y subsidiaridad legal de los agentes que intervienen en la cadena de provisión. Todo esto, en un contexto global donde el uso masivo de datos, la inteligencia artificial o la deslocalización de las infraestructuras físicas y lógicas forman parte esencial de los servicios IoT.

"preocupa la seguridad de los usuarios e infraestructuras que utilizan plataformas IoT frente a las ciberamenazas debido a la escala y especificidades técnicas que acrecientan su exposición."

Por otro lado, preocupa la seguridad de los usuarios e infraestructuras que utilizan plataformas IoT frente a las ciberamenazas debido a la escala y especificidades técnicas que acrecientan su exposición. Asimismo, debe tenerse en cuenta que en 2018 la conectividad IoT evolucionará mediante la próxima generación móvil 5G, caracterizada por la integración de los servicios de teleco-

municaciones móviles en plataformas de red IP virtualizadas o SDN-NFV *(Software Defined Networking - Network Functions Virtualisation).* La virtualización de las arquitecturas *(network slicing)* y de las plataformas de red mediante el uso compartido (pool) de servidores de propósito general en las redes de telecomunicaciones añaden nuevos retos de seguridad, especialmente en aquellos ámbitos IoT asociados a servicios esenciales e infraestructuras críticas. Tanto los anteriores como los dispositivos y las plataformas IoT, especialmente las integradas en *cloud* públicos, serán objeto de ciberataques de alcance masivo en 2018 según indica Forrester Research.

Este complejo escenario ha disparado las alarmas de la UE y, partiendo del *Cibersecurity Package* de 2017, la Comisión pondrá en marcha durante 2018 distintas iniciativas para la armonización, estandarización, certificación e interoperatividad entre plataformas IoT en el marco del *Mercado Digital Único*. En el mismo sentido se han pronunciado el *European Telecommunications Standards Institute (ETSI)* encargado del desarrollo de estándares IoT, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y la Asociación Global para las Comunicaciones Móviles (GSMA), publicando recientemente sendos informes, que son referencias obligadas en materia de la ciberseguridad del IoT en Europa.

El Informe divulgado por ENISA a finales de noviembre de 2017 *(Baseline Security Recommendations for IoT),* marco de referencia europeo en los próximos desarrollos normativos y técnicos, está dirigido a autoridades comunitarias, reguladores nacionales, desarrolladores, fabricantes y personal encargado de la seguridad en las empresas que tiene por objetivo prevenir y mitigar los ciberataques contra el

IoT, prestando particular atención a las infraestructuras críticas. El Informe ofrece una taxonomía de amenazas, ataques y análisis sobre las debilidades de IoT (gap analysis) y plantea las siguientes recomendaciones en materia de seguridad IoT:

- Promover la armonización de directrices, iniciativas, estándares o regulaciones
- Concienciar a consumidores y empresas sobre los riesgos y medidas a adaptar
- Definir directrices de seguridad para el ciclo de vida de los desarrollos software (SSDLC) y hardware
- Acordar la soluciones interoperables válidas para la cadena de provisión del ecosistema IoT
- Promover incentivos administrativos y económicos en actividades de I+D+D, en campañas de comunicación a consumidores, etc.
- Implantar una gestión de la seguridad en todo el ciclo de vida de los productos y servicios IoT
- Establecer responsabilidades entre los distintos agentes que interviene en la cadena de valor de los productos y servicios IoT

En sus orientaciones sobre la seguridad del IoT de 31 de octubre ***GSMA IoT Security Guidelines***, la GSMA también ofrece recomendaciones detalladas desde una perspectiva de presente, haciendo referencia a los estándares actualmente disponibles con el propósito de promover una metodología en materia de seguridad, garantizando la adopción de mejores prácticas para la protección de la privacidad y seguridad durante todo el ciclo de vida del servicio en tres ámbitos:

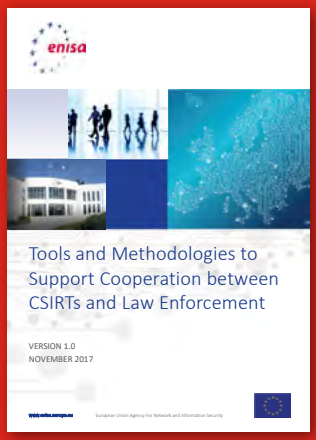
- el diseño de los ***ecosistemas IoT***
- el diseño y explotación de ***dispositivos IoT (end points)***
- los servicios de telecomunicaciones ***móviles orientados a IoT***, incluyendo tecnologías NB-IoT, LTE-M así como los estándares para uso de espectro licenciado con tecnologías de baja potencia 3GPP

En conclusión, a lo largo de 2018 la ciberseguridad de los dispositivos y plataformas IoT junto a la progresiva integración de éstas en entornos de cloud públicos van a demandar la ágil respuesta de todos los actores involucrados en el desarrollo armonizado de la interoperatividad, los estándares y las certificaciones, aspectos esenciales para asegurar una evolución escalable y sostenible del IoT en el ámbito de la ciberseguridad. En este sentido, los informes de ENISA y GSMA son una referencia obligada.

"2018 la ciberseguridad de los dispositivos y plataformas IoT junto a la progresiva integración de éstas en entornos de cloud públicos van a demandar la ágil respuesta de todos los actores involucrados en el desarrollo"

3 Informes y análisis sobre ciberseguridad publicados en enero de 2018

Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement (ENISA)



Stock taking of information security training needs in critical sectors (ENISA)

Cyber Maturity in the Asian-Pacific Region 2017 (ASPI)

China and Cyber: Attitudes, strategies and Organization (NATO CCD COE)

Cyber Crime Survey Report 2017 (KPMG)

Tendencias en Ciberseguridad 2018 (ESET)

Spain National Cyber Security Organization (NATO CCD COE)

2017 Internet of Health Things Survey (Accenture)

4 HERRAMIENTAS DEL ANALISTA:
The ThreatHunter-Playbook

El ThreatHunter-Playbook está orientado a ayudar al desarrollo de técnicas de elaboración de hipótesis para campañas de búsqueda de indicadores de amenazas mediante el aprovechamiento de registros de eventos de Sysmon y Windows. Este proyecto opensource proporciona cadenas de eventos específicos exclusivamente a nivel de host para que puedan tomarse y desarrollar la lógica necesaria para implementar consultas o alertas en las herramientas de seguridad existentes o en el formato preferido, como Splunk, ELK, Sigma, GrayLog, etc.

El repositorio sigue la estructura del framework MITRE ATT & CK que categoriza el comportamiento táctico de los adversarios posterior al punto de compromiso en grupos. Además, proporcionará información sobre las herramientas y plataformas de hunting desarrolladas por la comunidad de ciberseguridad para realizar pruebas y realizar los procesos de hunting en cualquier tipo de organización.

Los objetivos principales perseguidos por el proyecto son:

- Acelerar el desarrollo de técnicas de elaboración de hipótesis para campañas de hunting.
- Ayuda a los analistas de amenazas a comprender los patrones de comportamiento observados durante la post-explotación.
- Reducir el número de falsos positivos durante la búsqueda proporcionando más contexto entorno a los eventos sospechosos.
- Proporcionar suficientes recursos para ayudar en el desarrollo de un marco de hunting básico para la comunidad de ciberseguridad.
- Compartir conceptos y técnicas de búsqueda con otros usuarios de la comunidad.

5 Análisis de los Ciberataques del mes de enero de 2018

AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.

CIBERCRIMEN

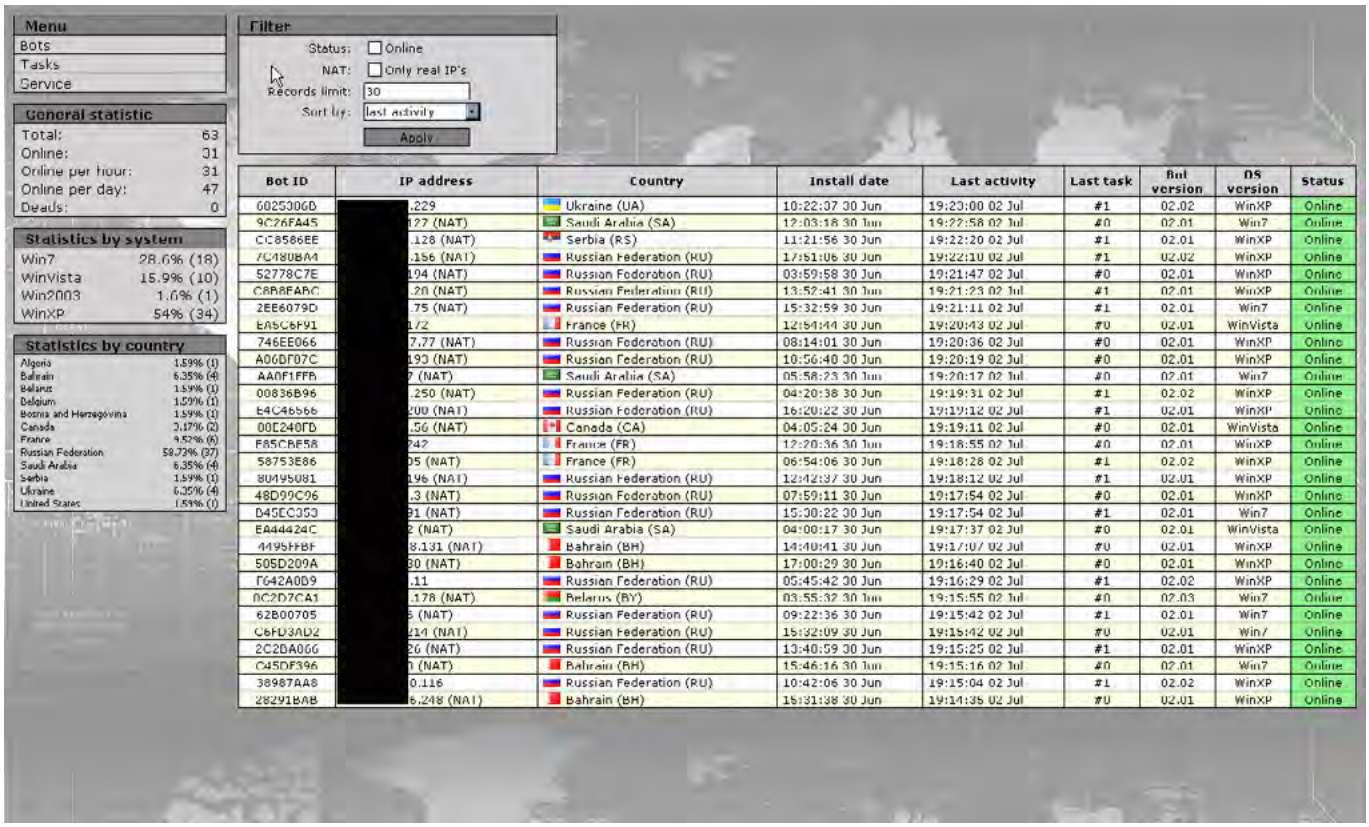
A comienzos de mes, *PayPal notificó públicamente que la información personal de cerca de 1,6 millones de sus clientes* podría haberse visto afectada por la filtración llevada a cabo por un actor que atacó las redes del proveedor de comunicaciones TIO Networks. A principios de noviembre, PayPal anunció que TIO había suspendido temporalmente sus operaciones después de que una investigación descubriera vulnerabilidades de seguridad en la plataforma de TIO. La investigación reveló que se había producido una brecha de seguridad afectando servidores que almacenaban la información de clientes y clientes de TIO. Si bien ni Paypal ni TIO han especificado exactamente a qué información han accedido los atacantes, sus declaraciones sugieren que los datos de la tarjeta de crédito y números de la Seguridad Social pueden haberse visto comprometidos.

Siguiendo los procedimientos regulatorios existentes, es de esperar que los usuarios afectados por la brecha sean contactados directamente y se les ofrezcan servicios de monitorización de crédito.

El 29 de noviembre de 2017, la Oficina Federal de Investigaciones (FBI), en estrecha cooperación Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), la Joint Cybercrime Action Task Force (J-CAT), Eurojust y socios del sector privado, desmantelaron una de las más familias de malware más prolíficas y extendidas llamada Andrómeda (también conocida como Gamarue).

Este malware ampliamente distribuido creó una botnet llamada Andrómeda. Según Microsoft, el principal objetivo de Andrómeda era distribuir otras familias de malware. La botnet Andrómeda ha estado desplegando más de 80 familias de malware distintas y, en los últimos seis meses, se ha detectado infectando un promedio de más de 1 millón de máquinas cada mes. Andrómeda fue utilizada también en la conocida red Avalanche, *desmantelada en una enorme operación internacional en 2016.*

Durante la operación se cerraron al menos 1.500 dominios y direcciones IP utilizados por los servidores de mando y control de la botnets (C&C) y cerca de 464 sub-botnets diferentes. Entre los programas maliciosos diseminados por Andrómeda se encuentran el prolífico ransomware Petya y Cerber, el bot Neutrino para ataques DDoS y los infostealers Ursnif, Carberp y Fareit.



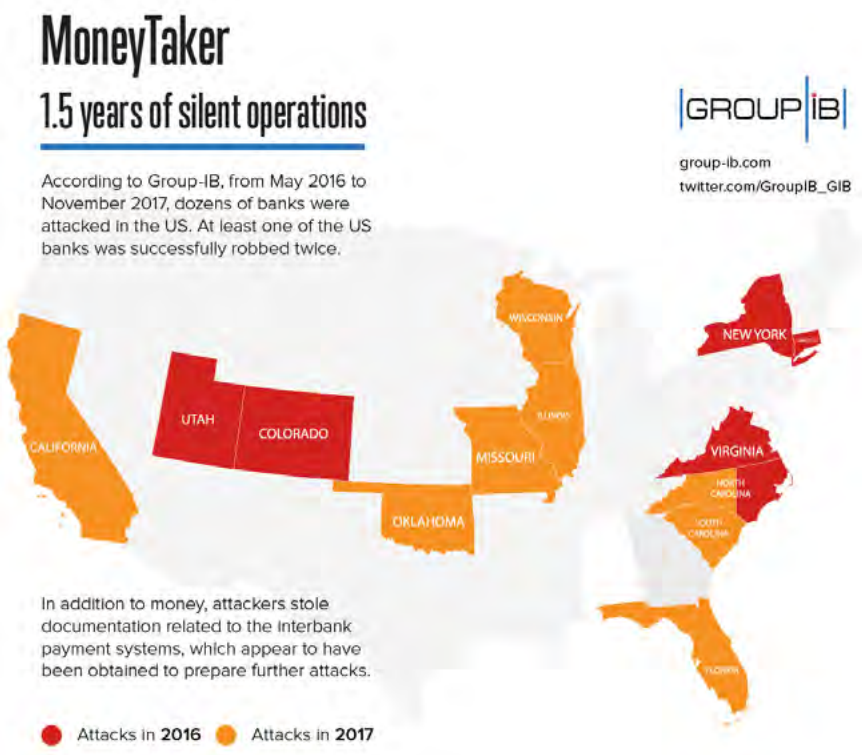
Panel del servidor C&C de la botnet Andrómeda

Diversos investigadores han advertido sobre la aparición de una nueva variante del malware para ejecutar ataques de denegación de servicio distribudio (DDoS) basado en Mirai a principios de mes, llamado Satori. La botnet Sartori fue detectada realizando escaneos masivos sobre los puertos 37215 y 52869 desde más de 280.000 direcciones IP únicas en un único día. Satori presenta algunas diferencias frente a Mirai y otras de sus variantes que descargaban un componente que realizaba escaneos de servicios Telnet para encontrar otras víctimas e infectarlos. Satori no usa un escáner sino que utiliza dos exploits embebidos que intentan conectarse a dispositivos remotos en los puertos 37215 y 52869. Esto hace que Satori sea definido como un gusano de IoT al propagarse a sí mismo, afectando principalmente a dispositivos IoT basados en Linux.

Los investigadores especulan sobre la repentina y rápida proliferación de Satori, apuntando a que pueda deberse a la explotación de una vulnerabilidad de día cero aún no identificada. Mirai ha sido modificado y desplegado por varios actores desde que se publicó su código fuente el 30 de septiembre de 2016.

Un grupo criminal desconocido ha sido capaz de, durante más de un año, sustraer aproximadamente 10 millones de dólares de bancos en Rusia y EEUU. *El grupo, denominado „MoneyTakers"*, se centró en bancos regionales pequeños con medidas de seguridad más laxas. Algunas actividades recientes también sugieren que el grupo podría estar preparándose para nuevos ataques en América Latina y, potencialmente, atacar los sistemas SWIFT.

Activo por lo menos desde el mes de mayo de 2016, el grupo se adiestró en los sistemas de pago con tarjeta de bancos comunitarios pequeños norteamericanos antes de atacar los sistemas transaccionales de bancos rusos. Los atacantes abrían cuentas e inhabilitaban los límites de retirada de efectivo en tarjetas de crédito legítimas, luego empleaban mulas para sacar la mayor cantidad posible de múltiples cajeros automáticos. Las tácticas de MoneyTakers reflejan una tendencia cada vez más extendida los grupos de cibercriminales que dirigen sus ataques contra los bancos en lugar de contra sus clientes, ya que las mejoradas medidas de seguridad hacen que los ataques contra los individuos sean menos rentables.



CIBERESPIONAJE

Un *informe de inteligencia publicado a mediados de mes* reveló que un grupo denominado APT 34 potencialmente vinculado a Irán ha pasado varios años infiltrándose en organizaciones industriales e infraestructuras críticas en varios países de Medio Oriente.

El informe expone el detalle de la campaña, que ha estado activa desde 2015. Los objetivos se alinean estrechamente con los países y entidades que tienen relaciones diplomáticas adversas con Irán. El informe también señala que los actores inician sesión en redes privadas virtuales (VPN) desde direcciones IP iraníes, se adhieren al horario normal de trabajo iraní y ocasionalmente han filtrado direcciones y números de teléfono iraníes. El grupo se dirige e infiltra a las organizaciones a través de su vasto y complejo uso de operaciones en redes sociales. Mediante ingeniería social se localizaban individuos con acceso a redes críticas. Una vez dentro de las mismas, APT 34 empleaba macros maliciosas de Excel y exploits basados en PowerShell para realizar movimientos laterales.

Identificada como una amenaza persistente avanzada, cabe destacar que las actividades de APT34 coinciden con un marcado aumento de las actividades, sofisticación y difusión de actores estatales iraníes, incluido el recientemente designado APT33, que sugiere que los actores basados en Irán están dedicando esfuerzos y recursos para desarrollar y mejorar sus capacidades de ciberespionaje. APT33 centra sus esfuerzos en entidades financieras, energéticas y gubernamentales; su objetivo es la infraestructura ICS, en particular, demuestra un interés relevante en el sector energético, que depende de numerosos sistemas industriales como parte de sus operaciones comerciales. Teniendo en cuenta la creciente.

Una *investigación realizada durante algo más de un año* sobre una campaña de ciberespionaje ha revelado que las agencias vinculadas al gobierno etíope usaron spyware comercial para monitorizar las actividades de disidentes y periodistas fuera del país. La investigación reveló que la campaña estaba dirigida contra periodistas, abogados, activistas y académicos en Estados Unidos, Canadá y Alemania. Los investigadores pudieron realizar una ingeniería inversa del malware utilizado en los ataques de suplantación de identidad y determinar que el spyware utilizado por Etiopía provino de Cyberbit Solutions, una subsidiaria de la compañía de seguridad nacional Elbit Systems, con sede en Israel.

Cyberbit es una de varias compañías cuyos productos han sido usados por regímenes autocráticos para monitorizar disidentes políticos y periodistas entre otros. Otras herramientas comerciales similares son ofrecidas por Hacking Team, Finfisher y NSO Group.

THIBER ya ha informado ampliamente en el pasado sobre el uso creciente de herramientas de espionaje y vigilancia comerciales, que ofrecen una solución de vigilancia atractiva y asequible para aquellas naciones que carecen de los recursos para desarrollar sus propias tecnologías. La legalidad de la comercialización y el uso de tales herramientas todavía no está claramente definida y varía de una nación a otra.

A mediados de mes, el Ministerio de Defensa indio contactó a sus soldados establecidos cerca de la frontera con China, solicitando que eliminasen de sus terminales todas las aplicaciones móviles desarrolladas en China de sus terminales. Según el *informe de inteligencia indio*, dichas aplicaciones transmiten datos del usuario y del terminal a servidores ubicados en China, pudiendo ser utilizados por el gobierno y el ejército chino para determinar su ubicación al otro lado de la frontera.

El informe referenciaba 42 aplicaciones de Android e iOS que los funcionarios recomendaron a los soldados eliminar, incluidas aplicaciones populares como Weibo, Wechat, UC Browser y CM Browser. El aviso fue enviado a los soldados estacionados en la Línea de Control Real (LAC), un área disputada en el norte de la India donde aún tienen lugar conflictos esporádicos, la última vez el verano pasado en la región de Doklam.

Aunque India suele ser víctima habitual ciberataques de grupos estatales pakistaníes, es esperable que grupos de espionaje vinculados al gobierno chino busquen nuevas formas de rastrear los movimientos de tropas a lo largo de la disputada LAC entre China y la India. El enfoque en el malware móvil indica un gran interés en rastrear los movimientos de las tropas a través de servicios de geoposicionamiento, incluso utilizando aplicaciones muy populares y conocidas como Weibo y Wechat para proporcionar legitimidad, tratando de pasar inadvertida.

Finalmente, la agencia de inteligencia alemana (BfV) emitió en diciembre un informe manifestando la detección de perfiles falsos de origen chino en LinkedIn usados para reunir información sobre funcionarios y políticos alemanes. Las autoridades afirman que hasta 10.000 funcionarios alemanes están siendo atacados, posiblemente en un intento de obtención de información relevante. El director del BfV alemán, Hans-Georg Maassen, afirmó que este acto representa un intento de infiltrarse en parlamentos, ministerios y agencias gubernamentales alemanes por parte del gobierno chino.

El informe publicó ocho de los perfiles más activos utilizados para contactar a los usuarios alemanes de LinkedIn. Están diseñados para atraer a los usuarios y promover jóvenes profesionales chinos que no existen. El BfV ha manifestado su preocupación por las tácticas cada vez más agresivas de ciberespionaje, incluyendo los intentos de injerencia en las elecciones parlamentarias de septiembre pasado.

Las redes sociales, y LinkedIn en particular, son frecuentemente utilizados por los actores de ciberespionaje para realizar investigaciones sobre objetivos potenciales que les permitan elaborar correos electrónicos de spear phishing muy sofisticados (por ejemplo) y otras formas de ingeniería social.

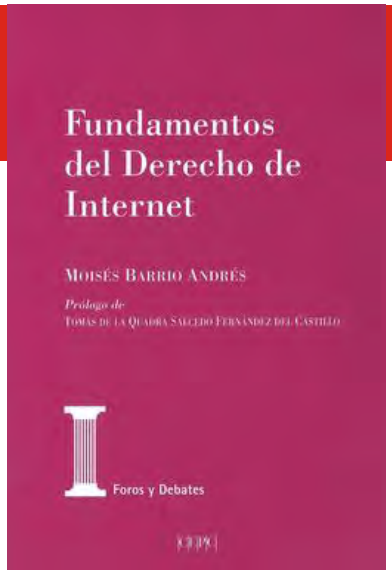
Imagen: Hans-Georg Maassen

6 Recomendaciones

6.1 Libros y películas

Libro:
INTELIGENCIA ARTIFICIAL: LO QUE TODO EL MUNDO DEBE SABER

Autor: Jerry kaplan
Num. Paginas: 192
Editorial: Teell Editorial
Año: 2017
Precio: 22,00 Euros
Sinopsis: En el transcurso de las décadas venideras, la Inteligencia Artificial tendrá un profundo impacto sobre la forma en que vivimos, trabajamos, hacemos la guerra, jugamos, buscamos pareja, educamos a nuestros jóvenes y cuidamos de nuestros mayores. Es probable que aumente en gran medida nuestra riqueza colectiva, pero también cambiará drásticamente nuestro mercado de trabajo, trastocará nuestro orden social y forcejeará con nuestras instituciones privadas y públicas. En última instancia, es posible que modifique cómo vemos nuestro lugar en el universo, a medida que las máquinas sigan avanzando en terrenos que previamente se consideraban dominio exclusivo de los seres humanos. En Inteligencia artificial – Lo que todo el mundo debe saber®, Jerry Kaplan explica los complejos asuntos relativos a la IA en un lenguaje claro y nada técnico. ¿Podrán realmente las máquinas superar a la inteligencia humana? ¿Cómo influirá la IA en nuestros trabajos y nuestros ingresos? ¿Puede un robot cometer un crimen voluntariamente? ¿Puede una máquina ser consciente o ejercer su libre albedrío? Muchos sistemas de IA actualmente aprenden de la experiencia y emprenden acciones que exceden las miras de su programación inicial. Como tales, generan cuestiones problemáticas para la sociedad. ¿Se le debe permitir a tu robot personal que te guarde la cola, o forzársele a testificar contra ti en un juicio? ¿Eres tú el único responsable de sus acciones? ¿Se les debe garantizar alguna vez a los robots el derecho a tener propiedades o a firmar contratos? Si llega a ser posible transferir nuestra mente a una máquina, ¿seguiremos siendo nosotros mismos? Las respuestas puede que te sorprendan.



Libro:
FUNDAMENTOS DEL DERECHO DE INTERNET

Autor: Moisés Barrio Andres
Num. Páginas: 533
Editorial: Centro de Estudios Politicos y Constitucionales
Año: 2017
Precio: 38,00 Euros
Sinopsis: "Fundamentos del Derecho de Internet" nace de una evidente constatación: la de que el fenómeno de Internet está provocando en el ámbito del Derecho transformaciones de hondura equivalente a las que, en general, viene produciendo en todas y cada una de las facetas de la vida social y del propio mundo digital, hasta el punto de integrar una disciplina autónoma, el "Derecho de Internet". La obra parte del concepto y caracteres de Internet, así como de sus bases históricas y estructurales, para examinar después las bases normativas e institucionales del Derecho de Internet, abordando el problema de su regulación, los principios generales de esta disciplina, las instituciones de gobernanza y coordinación de la Red, los instrumentos normativos y su propio contenido. Por todo ello, es una completa obra para conocer el Derecho de Internet, ofreciendo una visión comprensiva, clara y sistemática de su estructura general y problemas, incorporando también criterios que puedan ser aplicados al caso concreto y a la práctica en los tribunales. Así las cosas, el libro resulta de mucha utilidad para profesionales de las áreas jurídica y tecnológica, como a lectores del público en general teniendo en cuenta el enorme y creciente impacto del Derecho de Internet en la vida cotidiana.

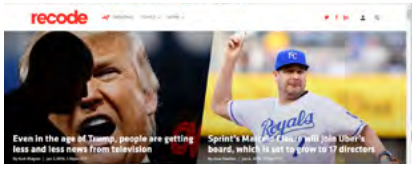
Libro:
LA SOCIEDAD DE COSTE MARGINAL CERO

Autor: Bernard Marr
Num. Paginas: 224
Editorial: Teell Editorial
Año: 2016
Precio: 20,00 Euros
Sinopsis: Hay un gran alboroto en torno al Big Data todos necesitamos saber qué es y cómo funciona. Pero lo que en realidad le diferenciará a usted del resto es saber cómo emplearlo para lograr resultados empresariales consistentes y que se correspondan con el mundo real, y ponerlo en práctica para aumentar el rendimiento. Big Data le enseña a implementar las mismas prácticas que han llevado a cabo las empresas líderes para acceder a las nuevas dimensiones de la rentabilidad. Aprenderá, a partir de explicaciones claras e innumerables ejemplos, cómo utilizan las empresas de éxito, pequeñas y grandes, el modelo SMART para tomar la delantera S = Empezar por la estrategia. M = Medir parámetros y datos. A = Aplicar el análisis. R = Comunicar resultados. T = Transformar la empresa.

6.2 Webs recomendadas

https://www.cert.govt.nz/
Sitio web del CERT gubernamental de Nueva Zelanda

https://www.recode.net/
Sitio web dedicado a las ultimas noticias de la industria tecnológica.

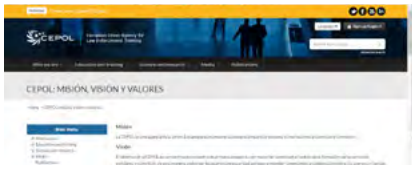


https://www.engadget.com/
Sitio web dedicado al análisis y evaluación de las últimas tendencias tecnológicas.

https://www.rand.org/about/people.html?topic=science-and-technology
Sitio web del think tank RAND dedicado a la ciencia y tecnología.

https://www.ccn-cert.cni.es/xjornadas-videos
Sitio web donde se alojan los videos de las X Jornadas STIC CCN-CERT

https://www.cepol.europa.eu/es
Sitio web de la Agenia Europea para la formación policial (CEPOL)



6.3 Cuentas de Twitter

@FalseFriends_es

@HackHispano

@DSMeu

@CCNPYTEC

@NCIAlibrary

7 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
10-12 enero	Zurich	IACR	Real World Crypto 2018	https://rwc.iacr.org/2018/
13 enero	Roma	BSIDES	BSides Rome	https://www.bsidesroma.it/
17-19 enero	St. Moritz, Suiza	Crypto Finance Conference	Crypto Finance Conference	https://www.crypto-finance-conference.com/en/
22- 23 enero	Kildare, Irlanda	Noord	CIO Ireland Dialogue	http://www.noordgroup.co.uk/itdleire/
23 enero	Madrid	ComputerWorld	ICT Trends 2018	http://eventos.computerworld.es/predictions/ict-trends
22- 24 enero	Madeira, Portugal	ICISSP	4th International Conference on Information Systems Security and Privacy (ICISSP)	http://www.icissp.org/
23- 24 enero	Tel Aviv	Microsoft	BlueHat	http://www.bluehatil.com/
23- 24 enero	Lille, Francia	FIC	International Cybersecurity Forum (FIC 2018)	https://www.forum-fic.com/site/GB,C59984,I59984.htm?KM_Session=16a475a842846384221e0c966e9dba3a
23- 24 enero	Londres	CDANS	Cyber Defence & Network Security Conference	https://cdans.iqpc.co.uk/
20- 26 enero	Les Diablerets, Suiza	IdQuantique	The 'Coming-of-Age' of Quantum Cybersecurity	https://www.idquantique.com/winter-school-2018/
29- 31 enero	Tel Aviv	CyberTech	CyberTech Israel	https://www.cybertechisrael.com/

Patrocinadores

GOBIERNO DE ESPAÑA — MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

GOBIERNO DE ESPAÑA — MINISTERIO DE DEFENSA

GOBIERNO DE ESPAÑA — MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

GOBIERNO DE ESPAÑA — MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

ACERINOX · AIRBUS GROUP · ATLANTIC COPPER · BBVA

enagas · IBERDROLA · IBM · INDITEX

indra · CaixaBank · MUTUAMADRILEÑA · OHL

tecnalia Inspiring Business · RED ELÉCTRICA DE ESPAÑA · renfe · REPSOL

gasNatural fenosa · Santander · Telefónica

Consejo Asesor Empresarial

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA · endesa · CEPSA

IBERIA · Fundación Cajasol · Escribano Mechanical & Engineering

Empresas Colaboradoras

CLH · European Climate Foundation · Aeroespacial y Defensa everis

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269