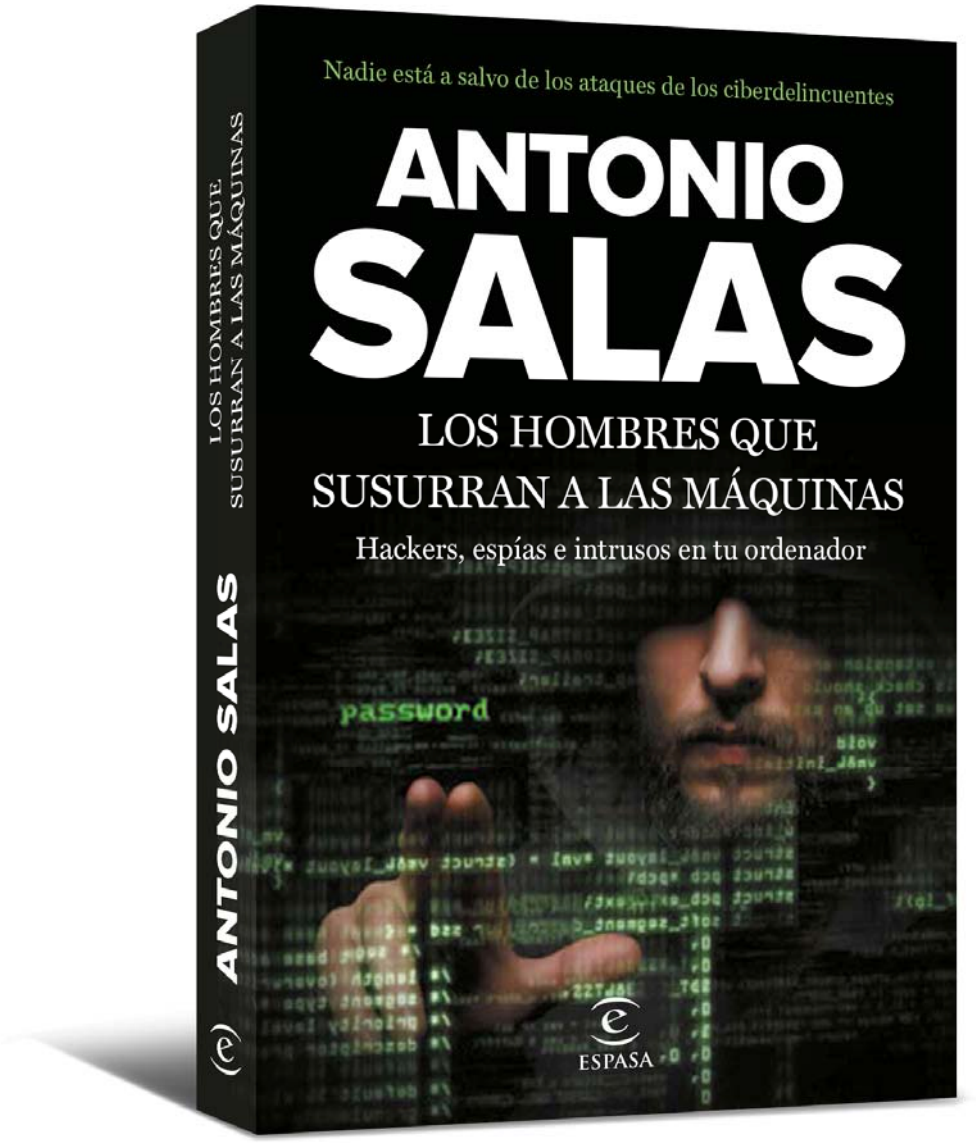
ESPASA

Una inquietante investigación en la que aprenderás cómo defenderte en la red. Una red en la que todos estamos atrapados. Una red llena de mentiras.



Los hombres que susurran a las máquinas

Hackers, espías e intrusos en tu ordenador

ANTONIO SALAS

Editorial Espasa • Fecha de publicación: 24 noviembre 2015
552 páginas • Tapa dura • 15x23 cm.
ISBN 978-84-670-4621-2 • Precio: 19,90 Eur

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

ESPASA

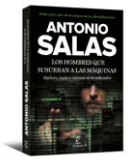
Los hombres que susurran a las máquinas

Hackers, espías e intrusos en tu ordenador

ANTONIO SALAS

No había otro tema posible. Después de dos años de investigación, Antonio Salas por fin ha podido cruzar las fronteras de un mundo hermético: el de los hackers. De rabiosa actualidad, esta investigación no dejará indiferente a nadie: todos somos víctimas.
Salas arremete con información contrastada sobre los peligros y vulnerabilidades de la red y de los modos para protegernos: hackers, crackers, espionaje, intrusos en tu ordenador y smartphone, perfiles falsos, ataques de cyberdelincuentes, cyberdefensa, deep web, whitehats, cyberterrorismo, estafas, kacktivismo, cyberjusticia, cyberbullying, el Internet de las cosas, en definitiva, el hacking en el siglo XXI. UN LIBRO PARA NO CERRAR LOS OJOS.

«Dicen los expertos que el Internet que utilizamos los usuarios de a pie —ese al que accedemos a través de buscadores como Google, Yahoo— es solo el 4% del Internet real. Es decir, que más del 96% de lo que hay en la red no aparece en esos buscadores».



Mientras te sientes seguro en la intimidad de tu cuarto, o con tu teléfono móvil en el bolsillo, se producen un millón y medio de ataques informáticos al día. La mayoría de nuestros teléfonos y ordenadores ya están infectados. Los ladrones de vidas buscan suplantar tu identidad en redes sociales, acceder a tus fotos y vídeos, utilizar tu red wifi y tus correos para cometer delitos que la Policía te atribuirá a ti... Pero eso solo es la punta del iceberg…

«Y todavía crees que todo en la red es gratis. Aún no sabes que cuando algo es gratis en la red, el producto eres tú».

Durante los últimos años he conocido a hackers de sombrero blanco, gris y negro, a ciberactivistas, ciberdelincuentes y ciberpolicías. He asistido a sus congresos, talleres y seminarios. He conocido a los espías que utilizan las redes informáticas para obtener información y a los ciberterroristas que distribuyen en ella su propaganda. He convivido con los ciberacosadores y con sus víctimas, e incluso me he convertido yo mismo en víctima de alguno de ellos. Y me he convencido de que, en el siglo XXI, no existe nada más urgente que conocer cómo funciona nuestra vida en la red. Porque todos estamos ya en ella. Héroes y villanos, criminales y policías, nazis, proxenetas, traficantes, terroristas… El ordenador, y más aún los teléfonos móviles, son nuestro pasaporte al nuevo mundo. Si no usas Internet y no tienes un teléfono móvil, no necesitas seguir leyendo. De lo contrario, prepárate para descubrir el lado oscuro, y también el más luminoso, de tu nueva vida. Una red en la que todos estamos atrapados. Una red llena de mentiras.

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

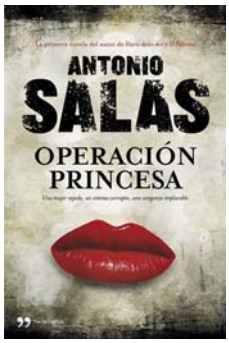
ESPASA

Antonio Salas es el seudónimo de un conocido periodista de investigación que debe mantener su identidad oculta desde que su primera obra, ***Diario de un skin,*** se convirtiera, debido a sus impresionantes revelaciones, en el libro más vendido en España durante el año 2003.

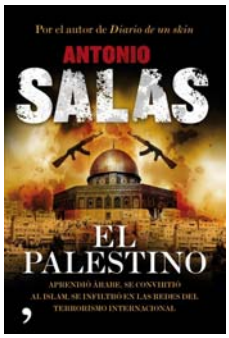
Testigo protegido de la Fiscalía, su testimonio fue vital para conseguir el primer fallo judicial contra un grupo neonazi en Europa: Hammerskin. Su infiltración en ***El año que trafiqué con mujeres*** facilitó de nuevo evidencias a la Policía española sobre los amos de la prostitución y motivó actuaciones del Gobierno mexicano sobre la trata de niñas chiapatecas.

En ***El Palestino*** recogía la información recabada en sus seis años de infiltración en organizaciones terroristas islámicas de trece países, bajo la identidad ficticia de Muhammad Abdallah, y donde llegó a convertirse en hombre de confianza del terrorista Carlos, El Chacal. Por dicho libro fue condenado a muerte por varias organizaciones armadas. En ***Operación Princesa,*** su última obra publicada, Salas recurrió a la narrativa para contar con libertad todo aquello que había visto durante su investigación sobre la corrupción y el narcotráfico, infiltrado como «Motero 1%», y que, por su alcance, no podía ser desvelado en un ensayo.

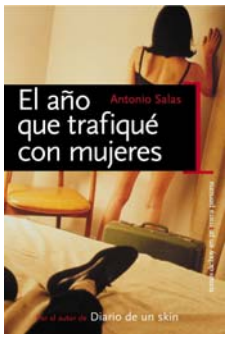
Más info en antonio-salas.com



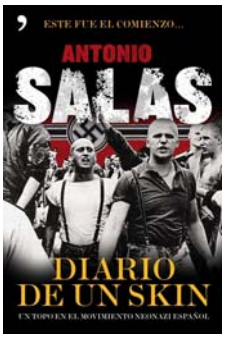
Operación Princesa
Temas de Hoy, 2013



El Palestino
Temas de Hoy, 2010



El año que trafiqué con mujeres
Temas de Hoy,



Diario de un skin
Temas de Hoy, 2003

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

ESPASA

2004

¿Buenos y malos?

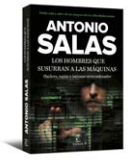
«La Policía está desbordada. De la misma forma en que la legislación contra nuevas drogas de diseño evoluciona al rebufo de la creatividad de los químicos**, los cibercriminales crean nuevos delitos que aún no están definidos como tales**».

«**Las nuevas leyes sobre seguridad informática tardan mucho en ser aprobadas**, y para cuando se legisla sobre un nuevo tipo de ciberdelito, intrusión o *malware,* los *blackhats* ya han inventado mil nuevos virus, gusanos, troyanos y han descubierto nuevas vulnerabilidades en la red. **Es una carrera perdida**».

Existen maneras de protegerte. Aunque solo ellos pueden ayudarnos a recuperar nuestras vidas robadas o evitar que nos las roben. Los hackers.

«La buena noticia es que **existen formas de ponérselo difícil**. Existen maneras de protegerte. De evitar ser una sardinilla anónima en un inmenso banco de peces. Aunque solo ellos pueden ayudarnos a recuperar nuestras vidas robadas o evitar que nos las roben. **Los hackers**».

Una nube de secretos



«Los secretos más inconfesables, las cuentas bancarias de los corruptos, la correspondencia más comprometedora de los políticos, los proyectos militares más confidenciales… **Toda esa información está aquí, a nuestro alrededor, suspendida en el aire, cifrada o no, en redes inalámbricas que nos atraviesan en todo momento y lugar**. Vivimos envueltos, rodeados, sumergidos en esa nube de información invisible. **Solo hace falta saber cómo abrir los ojos para descubrirla**».

Un hacker es todo lo contrario a un ciberdelincuente. Un hacker es un investigador tecnológico, un creador… un hombre que habla con las máquinas.

«—¿Así que ahora quieres conocer el mundo de los hackers? —me preguntó [el agente David R. Vidal] sentado tras las pantallas, sonriendo con la ironía y paternalismo al que ya me tiene acostumbrado—. ¿Y qué parte exactamente?
—¿Cómo que qué parte? Pues no sé… ¿hay más de una?
David negó con la cabeza, en un gesto que le he visto hacer en muchas ocasiones. Cada vez que le preguntaba una estupidez.
—***Phreaking,* ingeniería inversa, *hacking wifi,* ingeniería social, forense, *pentesting, exploits,* hacktivismo**… Pero ¿tú qué crees que es un hacker?
—¿Un pirata informático? —respondí haciéndome eco de un prejuicio repetido en miles de películas, informativos y artículos periodísticos.
—Mal empiezas. Si pretendes acercarte a la comunidad hacker insultándolos, no te van a recibir bien. **Un hacker es todo lo contrario a un ciberdelincuente. Un hacker es un sabio, un investigador tecnológico, un creador… un hombre que habla con las máquinas.**

Para más información y entrevistas con el autor:

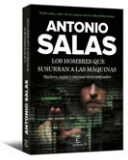
Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

—Pero todas las noticias que salen cada día sobre hackers…
—Eso es culpa de vosotros, los periodistas, que necesitáis titulares llamativos y frases sencillas en artículos asequibles. **Pero el mundo de la seguridad informática, en el siglo XXI, no es sencillo ni asequible. Es inmenso. Global**. Afecta a todo y a todos, y no se puede resumir en un titular periodístico. Ni siquiera en un libro.

[…]

A medida que David desarrollaba su argumentación, empecé a sentir temor.
—La mayoría de la gente pulsa en el primer botón que le ponen delante en una web, lo que equivale a suicidarse. **Los más torpes ni siquiera tienen antivirus, que sin ser una panacea es algo muy recomendable**.
Yo asentí con la cabeza sin añadir nada.
—Y los que tienen antivirus se creen que con eso basta. Y se equivocan. Ahora los ataques llegan de todos lados. No solo de la creciente industria del cibercrimen, que ya mueve más pasta que el tráfico de armas o la prostitución. A ellos les interesa todo lo que hay en tu ordenador: datos bancarios, fotos, vídeos, cuentas de email… Todo vale dinero. Pero también interesa lo que hay alrededor. Tu conexión wifi, tu módem, también puede emplearse para cometer un delito que luego te vas a comer tú. Por no hablar de tu teléfono móvil. **La industria del *malware* está creciendo más en el desarrollo de ataques a teléfonos móviles que a ordenadores**, y eso es porque ahora llevas tu vida en el móvil. Cuentas de Facebook, Twitter, WhatsApp, facturas… todo convenientemente geolocalizado en cada momento. Y tu vida vale dinero. Por eso te la roban».

El único ordenador seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento.



«Gene Spafford, profesor universitario de ciencias computacionales y experto en seguridad informática, dijo: «**El único ordenador seguro es aquel que está apagado y desconectado**, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él». Y Spafford estaba cometiendo el error de confiar en la lealtad de los guardias… No hay garantías».

Hackers y crackers

«**Un hacker es un investigador y un cracker es un delincuente informático**. Y dentro del crimen organizado, ahora están reclutando a muchos chavales, expertos en informática, para utilizarlos dentro del cibercrimen».

Un hacker es un investigador y un cracker es un delincuente informático.

[Conversación con **Israel Córdoba, *bussines-hacker***:]
—La ciberdelincuencia está creciendo. **España es el tercer país con mayor impacto de la ciberdelincuencia.**
—¿Como víctimas o como generador del delito?
—Como ambas cosas. Cuando se va a generar un ataque, lo que buscan es un país donde no haya acuerdos de colaboración. […] El panorama era desalentador. Todas las estadísticas oficiales y privadas coinciden en que **durante los últimos diez años el número de ciberataques crece proporcionalmente año a año**. El

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

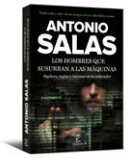
problema es que muchos de ellos se realizan desde otros países, donde la legislación no ampara a las víctimas del país receptor del ataque. Y ni siquiera es necesario que el delincuente se encuentre físicamente en el país donde están los servidores informáticos que lanzan la agresión, lo que complica todavía más la investigación.

—¿Y la administración? Supongo que igual que gastan nuestros impuestos en asfaltar carreteras o poner alumbrado, deberían preocuparse de las autopistas de la red…

—**La administración tendrá que poner medios y gastarse el dinero**. Antiguamente los bancos ponían un guardia jurado en la puerta, que ahora ha sido sustituido o complementado con cámaras. Ahora no basta con tener un ordenador bonito y que funcione bien. Debes tener otro equipo dedicado a la seguridad informática. Los diseñadores de programas y equipos se han concentrado en la operatividad de los sistemas, en que sean intuitivos, fáciles de manejar, que naveguen rápido… pero descuidaron la seguridad.

Por si acaso, al final tapé con un trozo de celo la webcam de mi ordenador. No lo he quitado desde entonces.

"Esa misma tarde me compré un antivirus, actualicé los servicios de Internet y contraté una VPN. También **aprendí a buscar el candado que aparece en el navegador**, y el encabezado https en lugar del http, al entrar en mi cuenta bancaria. Israel me explicó que ese candado y el protocolo https implican el cifrado de mis operaciones y por tanto mi seguridad. Pero ni con todo eso me sentí más seguro. Por si acaso, **al final tapé con un trozo de celo la webcam de mi ordenador. No lo he quitado desde entonces**».



«El **Big Data o procesamiento masivo de datos** es la nueva tendencia en la red. Ante el torrente brutal y gigantesco de datos que manejan los proveedores de Internet, las tecnologías de la información y la comunicación comenzaron a desarrollar técnicas para la captura, almacenamiento, búsqueda y análisis de esa ingente cantidad de datos con objeto de rentabilizarlos publicitariamente, como análisis de negocio, para control social o espionaje».

Cuestión de Estado

«Es probable que la Administración Obama jamás hubiese confesado las torturas y asesinatos cometidos en **Guantánamo o Irak**, de no haber sido porque Wikileaks filtró previamente miles de documentos, fotos y vídeos demostrándolo. **Es posible que jamás hubiésemos conocido la contabilidad del Partido Popular si Anónymous no la hubiese hecho pública**, antes incluso de que el juez Ruz hubiese concluido la instrucción del caso Bárcenas. Y estoy seguro de que jamás descubriríamos que los servicios de Inteligencia pueden captar todos nuestros emails, wasaps, conversaciones telefónicas y videoconferencias, si **Edward Snowden** no nos hubiese revelado cómo, dónde y cuándo lo hacen».

Es posible que jamás hubiésemos conocido la contabilidad del Partido Popular si Anónymous no la hubiese hecho pública.

«Lo que se estaba gestando en aquellos momentos [en marzo de 2014, mientras se celebraban por toda España las marchas de la dignidad] en los despachos del

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

Gobierno de España era una **remodelación total de la Ley de Seguridad Ciudadana**, que afectaría de forma demoledora a nuestras libertades. No solo en las calles. También en la red. Y yo tendría el privilegio de seguir el proceso tal y como lo vivió la comunidad hacking».

«Aquella noche, año y medio antes de que se aplicase la Ley Mordaza, fui testigo de cómo **varios miembros de las UIP intuían que habían sido «marionetas» del sistema, intencionadamente mal coordinados por sus superiores** para sufrir una brutal agresión que justificase un endurecimiento en las leyes de seguridad ciudadana.

—Lo hemos comentado muchos compañeros, Toni. No fue normal. Nos enviaron al matadero para que nos forrasen a hostias, sabiendo que no teníamos ni la cobertura ni la equipación apropiada para ese operativo… Y muchos pensamos que lo hicieron para tener una **justificación gráfica que les permitiese endurecer la ley**… Fuimos su excusa».

Impotentes para detener a los hackers —que descubrieron que un invento de origen militar, Internet, podía emplearse contra los conspiradores que lo idearon—las agencias de Inteligencia decidieron que la mejor forma de combatir la información no deseada era mezclarla con desinformación.

«A partir de **julio de 2015, una fecha clave en la historia de la cultura hacker** también existirán corsarios autorizados por los gobiernos para utilizar armas y herramientas de hacking, que se considerarán ilegales en manos de los piratas. **Unos tendrán la autorización para realizar ataques**, para testar equipos, para explorar vulnerabilidades, dentro de los límites de la nueva ley. Los otros, los de siempre, continuarán moviéndose en la clandestinidad, al margen de la legalidad del momento, sin molestarse en pedir permiso al poder para utilizar tal o cual programa, aplicación o código en sus investigaciones tecnológicas. Explorando los nuevos sistemas en busca de sus errores, porque esa es su pasión. Sin embargo, a partir de julio de 2015, con la **entrada en vigor del nuevo Código Penal, cosas que antes no estaban penadas ahora pueden implicar prisión»**.

«Si yo quiero investigar a un usuario que ha colgado un vídeo donde dice que te van a matar, por ejemplo, ese vídeo está en YouTube y YouTube está en Estados Unidos. **Pero en España no existe una legislación que obligue a YouTube a darte esa información**. Y si no quieren darte esa información, no te la dan, te pongas como te pongas. De hecho, no lo hacen. Se pasan por el forro las peticiones policiales».

Ciberterrorismo islamista

«Los servicios de Información e Inteligencia tienen un problema a la hora de manejar información sobre lo que ocurre realmente en las mezquitas. Existen muy pocos funcionarios de las Fuerzas y Cuerpos de Seguridad del Estado que hablen árabe y/o sean musulmanes. Y menos aún dispuestos a infiltrarse en el terrorismo yihadista. La figura del agente encubierto y el agente provocador apenas están recién legisladas en España, y en un país tan garantista como el nuestro, las trabas legales para hacer ese tipo de investigación encubierta son enormes.

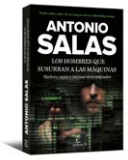
Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

En la era de la tecnología, el terrorismo no puede nutrirse solo con sangre. Necesitan algo más. **Necesitan que les demos vida en Internet. Nos necesitan a nosotros. Boko Haram lo descubrió entonces**, pero antes del siguiente Ramadán otro nuevo monstruo sin precedentes en la historia surgiría en la red. Un engendro tan blasfemo como Boko Haram pero con recursos, experiencia y voluntad infinitamente superiores. Y dispuestos a utilizar la red, en el nombre de Allah, como jamás se había utilizado antes.

Basta seguir los *hashtags* apropiados en Twitter para descubrir los perfiles de cientos de terroristas del ISIS, que constantemente invitan a los jóvenes musulmanes de Occidente a viajar a Siria para unirse a su aberrante causa.

Por la noche, en un cibercafé cercano al hotel [en Ceuta], seguí las indicaciones de Hakim para buscar al Diablo en la red. No fue difícil. **Basta seguir los *hashtags* apropiados en Twitter para descubrir los perfiles de cientos de terroristas del ISIS,** que constantemente invitan a los jóvenes musulmanes de Occidente a viajar a Siria para unirse a su aberrante causa. Una vez identificados los usuarios de esos perfiles, es fácil localizarlos también en Facebook y en otras redes sociales, y **asistir perplejo al espectáculo de horror que su delirio siembra en uno de los países más bellos y hospitalarios que yo he conocido**. Allí está su diabólica obra, asomándose a la pantalla de tu ordenador. Y su mensaje recurrente: ven a Siria, únete al ISIS.



Poco a poco, las primeras revistas yihadistas, que también podían descargarse en Internet, como *La Voz de la Yihad, Campo de entrenamiento Al Battar* o la destinada a las yihadistas mujeres *Al Khansaa,* combinaron sus contenidos con vídeos efectistas y atroces. Y todo porque **habían descubierto el efecto mediático del horror, y del eco que despertaba el enfermizo morbo de los seres humanos**, con las decapitaciones televisadas».

ISIS: terrorismo en línea

«Buena prueba de su capacidad de inventiva fueron las **primeras apps del Estado Islámico**, como Farachar, un sistema de mensajería telefónica vía Bluetooth. O The Dawn of the Glad Tidings («El amanecer de la Buena Nueva»): una aplicación para el control y sincronización de cuentas en Twitter.
No solo eso, además **desarrollaron sus propios videojuegos**. En una cultura tecnológica en la que los jóvenes crecen frente a las pantallas del ordenador, los yihadistas les ofrecieron cambiar el papel de héroes y villanos en sus videojuegos. Y además, les brindaban la posibilidad de sacarlos de la pantalla y jugar en la vida real. **Matando, decapitando, masacrando, como hacían en los juegos de ordenador, pero en el mundo físico**. En el frente de combate. El *meme* popularizado en las cuentas del ISIS, con la leyenda «Este es nuestro Call Of Duty y nosotros reencarnamos en el Paraíso» lo expresa perfectamente».

Matando, decapitando, masacrando, como hacían en los juegos de ordenador, pero en el mundo físico.
El *meme* popularizado en las cuentas del ISIS lo expresa perfectamente:
«Este es nuestro Call Of Duty y nosotros reencarnamos en el Paraíso».

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

«Para un público menos violento, desarrollaron además toda una estrategia de captación «blanda» a través de **páginas como Jihad Matchmaker, que buscaba emparejar con fines matrimoniales a jóvenes musulmanas con guerreros del ISIS**. O la campaña CatsOfJihad, protagonizada por **tiernos y entrañables gatitos**, ataviados como *mujahidin* o posando con los guerreros del Estado Islámico. Adorables».

«En los Estados Unidos, tras los atentados del 11-S los ciudadanos tuvieron que elegir entre seguridad y privacidad, y eligieron lo primero».

ETA en la red

«Según dicho reportaje [de la revista *Interviu* en febrero de 2009], Arkaitz Landaberea [informático del diario *Gara,* acusado de pertenecer a la banda desde 2006, y detenido durante la desarticulación del Comando Urruti] había escrito un **manual de hacking para terroristas, mucho antes de que Al Qaeda, Boko Haram o el Ejército Islámico** aprendiesen a gestionar la red. Y lo había hecho por orden de un viejo conocido: Francisco Javier López Peña, alias «Thierry», el jefe de ETA en aquel momento, que había sido detenido en Francia el 20 de mayo de 2008».

«Aunque inocuo, el **virus «anti-ETA»** hacía aparecer en la pantalla de los ordenadores infectados una mano blanca, símbolo de la protesta multitudinaria por la cruel ejecución del concejal de Ermua. Fue uno de los primeros virus hacktivistas de la historia. […] Es irónico, pero **los de ETA calificaron a los hackers que habían desarrollado el ataque como "ciberterroristas"**».

Suicidio digital

«Solo un imbécil puede creer a estas alturas que puede amenazar e insultar desde la red, y pretender que no le pillen».

«Algunas personas, en un momento determinado de su vida, deciden **desaparecer de manera voluntaria de la red borrando toda su vida digital**.
—La última solución, si todo falla, es el suicidio digital… —comenté.
—Depende —replicó [Selva María Orejón, fundadora y directora ejecutiva de OnBranding]—. No es «si todo falla». A veces nos han pedido desaparecer de Internet sin que se haya intentado nada antes. Quiero decir que, en ocasiones, el propio objetivo del cliente es desaparecer con la identidad que tenía y reaparecer con otra nueva. Un claro ejemplo son las personas **víctimas de violencia de género, personas que han estado en prisión, personas que han tenido un pasado vinculado a una historia de la que no se sienten orgullosos ni las beneficia, o bien personas que necesitan hacer un borrón y cuenta nueva, por seguridad»**.

Los *whitehats* de la Guardia Civil

«—Aunque vosotros no podáis aumentar recursos, el cibercrimen sí aumenta…
—Yo no lo tengo muy claro. —El capitán [César Lorenzana González es el jefe de la Sección de Investigación del Grupo de Delitos Telemáticos de la UCO] me

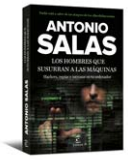
Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

sorprendió con su respuesta—. **No sé si el cibercrimen aumenta, o es que cada vez vemos más claro lo que hay**. Poco a poco vamos viendo la foto completa de todo lo que está ocurriendo, porque hasta hace cinco años nadie hacía informes de esto.
—Te oí comentar una vez, y me pareció genial, que **la pornografía infantil no existe**…
—No, de hecho **fuera de España no se le llama «pornografía», es abuso sexual infantil. Son violaciones de niños y bebés en toda regla**. La pornografía tiene otras connotaciones».

«Suplantar a alguien para abrir un Facebook no está tipificado como delito. Pero precisamente Jorge [Bermúdez, fiscal delegado de Delitos Informáticos en Guipúzcoa] nos dio la solución: **hackear la ley**. La falsedad en documento mercantil sí es delito. Me explico. La suplantación de identidad en Internet como tal no está regulado en el Código Penal, porque la usurpación de estado civil, que es el supuesto penal, habla de un acto jurídico formal, y publicar en Facebook no es jurídico y mucho menos formal. Pero **al abrir una cuenta en un portal de servicios, que para ofrecer ese servicio me obliga a aceptar unas condiciones de uso que yo firmo… eso a efecto jurídico es un contrato**. ¿Y qué estás haciendo? Firmando un contrato en nombre de otra persona. Eso es falsedad en documento mercantil… Entonces por ahí sí puedo meterle mano. […] Otra cosa por ejemplo, es que te roben la cuenta de PayPal. Eso es como robarte la tarjeta de crédito. Eso es un **fraude bancario y fraude económico. Es delito».**

«Ha cambiado el paradigma de la Policía: yo ya no estoy centrado en el delincuente, estoy centrado en la prevención. Si me das a elegir entre pillar a quince delincuentes o evitar una víctima, yo me quedo con evitar la víctima. Lo más importante es que esto se sepa y que las víctimas sepan cómo actuar».



Hacking WIFI

Más allá de los virus troyanos y gusanos, del robo de conexión al vecino, y del *phishing*, **el hacking wifi supone otra dimensión de nuestras vulnerabilidades**. Ya no es necesario tocar el ordenador de la víctima. Utilizando antenas direccionales […] es posible introducirse en un sistema desde un coche aparcado en la calle o desde el edificio de enfrente. O lo que es peor, acomodarse en un lugar público, como una terminal de un aeropuerto, el vestíbulo de un hotel o una estación de ferrocarril, y solapar la wifi gratuita legítima del lugar, con una señal que emite el atacante, y que bautizará con un nombre inocente: «wifi gratis», «Renfe», «wifi Barajas», «Hotel Ritz», etcétera.

Esteganografía: hacking para espías

«A diferencia de la criptografía, utilizada para cifrar o codificar información de forma que solo pueda ser descifrada por el receptor legítimo —por ejemplo los mensajes nazis de la máquina Enigma—, **la esteganografía oculta dicha**

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

información en un «portador», para que en caso de ser interceptado, nadie pueda sospechar que dicho portador oculta un mensaje. Como si el mensaje de la Enigma fuese escrito con tinta invisible en una hoja de periódico».

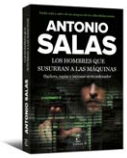
«Durante los últimos años los servicios de Inteligencia israelíes, británicos y norteamericanos han descubierto que, más allá del uso propagandístico de sus webs, la comunicación por cifrado PGP, o la compartición de buzones de correo, los terroristas habían desarrollado la estenografía para **transmitir mensajes ocultos, por ejemplo a través del porno, y webs abiertas como eBay o Reddit**. A la vista de todo el mundo».

La lista Falciani

«Hervé Falciani, el informático que hackeó a la banca suiza, me confesaría, por primera vez, que la **esteganografía había sido una de las herramientas que utilizó para sacar la información de la «Lista Falciani»** de los ordenadores del HSBC…"

«Entre los usuarios de las cuentas en la banca suiza filtradas por Falciani había políticos, jefes de **Estado, banqueros, empresarios… pero también narcotraficantes y terroristas. Todos protegidos por el inexpugnable secreto bancario**. Hasta que Falciani lo hackeó. Literalmente».

«Según me relató Falciani, Manuela Carmena y Ada Colau se habían puesto manos a la obra para intentar llevar a la práctica esos «sistemas de control a quienes desempeñen cargos públicos» de los que había hablado con Pablo Iglesias».



«Según me relató Falciani, inmediatamente después de ganar las elecciones municipales, el mes de mayo anterior, **Manuela Carmena y Ada Colau** se habían puesto manos a la obra para intentar llevar a la práctica esos «**sistemas de control a quienes desempeñen cargos públicos» de los que había hablado con Pablo Iglesias»**.

El negocio del malware

«La **industria del *malware* evoluciona a una velocidad de vértigo**, creando falsos servicios y apps que atacan nuestra intimidad, infiltradas entre las herramientas legítimas. […] El mejor ejemplo es la aplicación The Adult Player, una app —afirma el diario *ABC*— que promete contenido pornográfico gratuito a quien la descargue, y que en realidad, según se publicó en 2015, toma el control del teléfono móvil, te hace fotos con tu propia cámara contando con pillarte en alguna situación «comprometida» y subida de tono mientras ves las imágenes, y acto seguido te bloquea el teléfono y amenaza con subir las fotos a tus perfiles sociales si no pagas entre 440 y 500 euros».

«Lucas (genio informático fichado por una de las grandes compañías norteamercanas):
—Todos usamos la red. Pero la visión que tenemos de la tecnología los

Para más información y entrevistas con el autor:

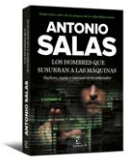
Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

profesionales y la que tenéis los usuarios todavía es muy diferente. A medida que pasen los años, y este terreno que os parece ignoto y misterioso sea más familiar, esa distancia se acortará. Pero ahora mismo es enorme. Por eso, cada vez que la comunidad lee las noticias que se publican sobre nosotros, nos morimos de risa. Periodistas, políticos, jueces…»

«Conseguir una herramienta peligrosa no es fácil. Necesitas dos ingredientes fundamentales para cocinar la diferencia entre el éxito y el fracaso: **vulnerabilidades del día cero**, es decir, aquellas vulnerabilidades que se descubren en los sistemas y que son tan recientes que todavía no se han solucionado, es decir que no hay «parches» disponibles. En el mercado negro, dependiendo de su importancia, **se pueden pagar tranquilamente cifras de 10.000 o 15.000 .** Estas vulnerabilidades solo duran días o semanas, porque más pronto que tarde se solucionan. Pues bien, cualquier hacker que conozca a tiempo una de ellas es el rey del mambo».

El Internet de las cosas (IoT, por las siglas en inglés de «Internet of Things») preocupa a la comunidad hacker.

«**El Internet de las cosas** (IoT, por las siglas en inglés de «Internet of Things») preocupa a la comunidad hacker. De hecho, en la mayoría de las CON se presenta al menos una conferencia que aborda este inquietante fenómeno. […] Montañas rusas que pueden ser hackeadas para provocar un accidente, impresoras que pueden incendiarse a distancia… En otras palabras, un ejemplo tras otro de cómo **los dispositivos electrónicos ya implantados en los niveles más íntimos de nuestra vida doméstica pueden volverse contra nosotros»**.



Anónymous y su #OpCharlieHebdo

El 7 de enero de 2015, se lastimó la libertad de expresión —dijo Anónymous—. Es nuestra responsabilidad reaccionar.

«Tras los atentados del 7 y 8 de enero [contra Charlie Hebdo], Anónymous declaró formalmente la ciberguerra al Estado Islámico. «**El 7 de enero de 2015, se lastimó la libertad de expresión —dijo Anónymous—. Es nuestra responsabilidad reaccionar**».

«Es importante comprender que **Anónymous no se parece a otros grupos hacktivistas históricos** como Network Liberty Alliance, milw0rm, Cult of The Dead Cow o los letales y divertidos Lulzsec. No es una organización, ni una asociación, ni siguiera un grupo estructurado. **Es una dinámica. Una corriente de pensamiento que fluye por la red** y en la que un número indeterminado de individuos, sin un rango, liderazgo o mando mayor que los demás, se dejan arrastrar para una acción determinada».
«No quedó ahí: en la nueva fase de su Operación Charlie Hebdo, a mi juicio más inteligente y perjudicial para los intereses del ISIS en la red, **Anónymous generó contenidos en los buscadores de Google para desplazar los referentes al Estado Islámico.** También establecieron un protocolo para que cualquier usuario de Facebook o Twitter pudiese localizar cuentas yihadistas y denunciarlas a Anónymous, la Policía o a los mismos responsables de la red social».

Para más información y entrevistas con el autor:

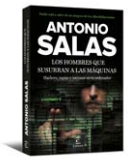
Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

Ciberguerra, ciberdefensa

«Ni la aviación, ni las bombas atómicas, ni los submarinos, ni ningún otro invento revolucionario aplicado a la guerra ha evitado que continúen existiendo los combates convencionales. Y en el siglo XXI el concepto ***ciberguerra*** viene a sumarse a esas nuevas tendencias, haciendo que algunos autores imaginen una futura guerra mundial sin fusiles, limitada a teclados de ordenador."

Anónymous generó contenidos en los buscadores de Google para desplazar los referentes al Estado Islámico. También establecieron un protocolo para que cualquier usuario de Facebook o Twitter pudiese localizar cuentas yihadistas y denunciarlas.

«La gente piensa que un barco aislado, en alta mar, es ciberinvulnerable… Pues no es verdad. **Un tipo en su casa, con un ordenador, podría interferir la conexión satelital de un barco**. En lugar de tirarle un torpedo se le puede hacer un ciberataque a través de la actualización de la cartografía digital, por ejemplo, mediante el cual se puede alterar el funcionamiento de la planta propulsora del barco. Es muy complicado, pero teóricamente posible».



«**España llegó tarde al campo de batalla, y pagaremos el precio**. Porque no solo nos unimos al encuentro hacia el final del segundo tiempo, sino que lo hacemos con unos recursos paupérrimos. Las austeras instalaciones del MCCD están a años luz del potencial, técnico y humano, con que cuentan grupos como el Batallón 77 británico».

«Después de la Kali Linux, conocí otras muchas [**herramientas diseñadas para explotar vulnerabilidades en un sistema], incluso de fabricación española**, como Foca, Anubis, etcétera. Y descubrí los embriagadores efectos del **torrente de adrenalina que desbordan las neuronas del hacker, cuando accede al interior de un sistema ajeno**: una universidad norteamericana, un servicio de Información, una poderosa multinacional, explorando sus puertos, sus impresoras, sus bases de datos, buscando una puerta de acceso al sistema, y encontrándola. Tan excitante como un *striptease,* pero más peligroso."

La gente piensa que un barco aislado, en alta mar, es ciberinvulnerable… Pues no es verdad. Un tipo en su casa, con un ordenador, podría interferir la conexión satelital de un barco.

Tor: el pasaporte a una ciudad sin ley

«TOR es una red de comunicaciones en la que el enrutamiento de los mensajes intercambiados entre los usuarios es cifrado, y **no revela la dirección IP de dichos usuarios**. TOR utiliza un software libre que funciona a través de una serie de *routers* donados por individuos y fundaciones para **proteger el anonimato de los internautas** y por tanto su libertad de actuación en la red».

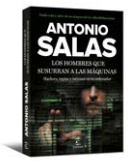
Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es

«TOR es el pasaporte que te permite viajar a una ciudad sin ley. Una ciudad en la que reina la anarquía y en la que todo está permitido. **Sin reglas, sin normas, sin autoridades que pongan límite a tus actos**. Una ciudad en la que puedes caminar por la calle indocumentado, y ocultando tu rostro tras un pasamontañas y tus huellas digitales con guantes de látex. ¿Imaginas un lugar así? Pues eso es la llamada **web profunda**…»

TOR es el pasaporte que te permite viajar a una ciudad sin ley. Una ciudad en la que reina la anarquía y en la que todo está permitido. Es probable que si buscas en ese tipo de páginas, te encuentres a tus propios hijos, sobrinos, nietos…

«Hasta para un simple usuario torpe y novato como yo **resultó sencillo encontrar páginas donde se ofrecían pasaportes, DNI y todo tipo de documentación falsa**, de prácticamente todas las nacionalidades del mundo. […] O cocaína, hachís, éxtasis, opio, ketamina, marihuana y **cualquier otro tipo de sustancia prohibida**, que continúan a disposición de los internautas, mucho después del cierre de Silk Road. […] Pero **lo peor de todo el viaje a TOR fue descubrir la nutrida, variada y prolífica presencia de la pedofilia** en todas sus manifestaciones imaginables».



«Es probable que si buscas en ese tipo de páginas, te encuentres a tus propios hijos, sobrinos, nietos… No porque nadie de la familia haya abusado de ellos sexualmente —aunque no sería el primer caso—, sino porque en algunas de esas páginas se compilan **esas fotos inocentes de tus hijas en la playa que subiste a Facebook**, esos vídeos de tu nieta bailando que tenías en tu disco duro cuando te lo crackearon (tú que dices que no tienes nada que pueda interesar a los ciberdelincuentes), o esas imágenes de tus sobrinos desnuditos sobre la colcha, en las que solo un enfermo mental puede ver un contenido sexual… pero es que esos enfermos mentales existen».

Pedofilia en la red

«[Según afirma en su tesis la inspectora Silvia Barrera], el **72% de las víctimas son niño/as entre 0 y 10 años de edad**. El 44% imágenes que representan violaciones y torturas sexuales sobre menores. El 48% de páginas web, comerciales o no, están **alojadas en servidores de América del Norte y el 44% en Europa y Asia**. Durante el año 2009 fueron cerrados 1.316 sitios web por contener material relacionado con abusos sexuales a menores».

«No puedo sacarme de la cabeza la imagen de Mario Torres, y de **las niñas mexicanas de diez, doce o catorce años que me vendía, a 25.000 dólares cada una,** en el restaurante de la plaza de Cubos, en pleno centro de Madrid. **Niñas «nuevitas» por las que «puedes cobrar lo que quieras»**. Mario conocía el negocio, y sabía que además de prostituyéndolas, esas niñas podrían generar miles de fotos y vídeos de contenido pedófilo, que adecuadamente gestionados, **podrían amortizar la «inversión» en cuestión de semanas»**.◆

Para más información y entrevistas con el autor:

Desirée Rubio De Marzo
Prensa y comunicación Espasa
Grupo Planeta. Josefa Valcárcel 42, 5ª planta - 28027 Madrid
T. 91 423 03 54 | M. 680 683 717 | drubio@planeta.es