LOS DELITOS DEL FUTURO

TODO ESTÁ CONECTADO
TODOS SOMOS VULNERABLES
¿QUÉ PODEMOS HACER AL RESPECTO?

MARC GOODMAN

Marc Goodman, una de las autoridades más destacadas en materia de seguridad mundial, conduce a los lectores a las profundidades del ciberespacio para mostrar cómo delincuentes, empresas e incluso gobiernos utilizan la tecnología contra el ciudadano, y cómo ello nos hace más vulnerables de lo que jamás habríamos imaginado.

Los avances tecnológicos nos han beneficiado de incontables maneras, pero tienen un lado oscuro: pueden volverse en nuestra contra. Los «hackers» son capaces de activar las cámaras de vigilancia y webcams de cualquier hogar, los ladrones leen las redes sociales para conocer nuestros hábitos y los acosadores toman el control de los GPS de los coches de sus víctimas para seguirlas allá donde se dirigen. Los delincuentes de hoy pueden robarnos la identidad, hacerse con los datos de nuestras cuentas bancarias y copiar el contenido de los servidores informáticos. Pero esto es sólo el principio. Los delincuentes del futuro podrán desactivar los frenos de un coche desde kilómetros de distancia, electrocutar a un portador de un corazón artificial, fabricar AK-47 con una impresora 3D o transportar droga a través de drones.

Los delitos del futuro es también un poderoso y útil manual de supervivencia online que nos da las claves para evitar riesgos, reforzar nuestro derecho a la intimidad y encarar el futuro desde la seguridad y el control sobre nuestros aparatos tecnológicos antes de que sea demasiado tarde.

Un libro que se lee como una novela de ciencia ficción pero que está basado en hechos científicos.

Lectulandia

Marc Goodman

Delitos del futuro

ePub r1.0
XcUiDi 01.12.16

Título original: *Future Crimes*
Marc Goodman, 2015
Traducción: Gemma Deza Guil

Editor digital: XcUiDi
ePub base r1.2

A todos mis profesores,
de los que tanto he aprendido

Prólogo

El optimista irracional: ¿porqué soy así?

Mi llegada al mundo de la delincuencia con altas tecnologías se produjo de manera inesperada en 1995, cuando, a mis veintiocho años, trabajaba como investigador y sargento en la famosa comisaría del Parker Center del Departamento de Policía de Los Ángeles. Un día, mi teniente bramó mi nombre desde el otro lado de la infestada sala de la brigada, donde reinaba el típico trajín: «¡Gooooooodmaaaan, mueve el culo hacia aquí!». Supuse que me había metido en algún lío, pero, en cambio, el teniente me formuló la pregunta que cambiaría mi vida para siempre:

—¿Sabes cómo se comprueba la ortografía en WordPerfect?

—Sí, jefe, pulsando Ctrl + F2 —respondí.

Me sonrió y dijo:

—Sabía que eras la persona a quien preguntar.

Y así empezó mi carrera como investigador de altas tecnologías, con mi primer caso de delincuencia informática. Saber cómo comprobar la ortografía en WordPerfect me situó entre la élite de policías con conocimientos tecnológicos de principios de la década de 1990. Desde aquel caso, he sido un ávido observador y estudiante tanto de las tecnologías como de sus usos ilícitos. Y aunque soy consciente del peligro y de la destrucción que puede conllevar su uso indebido, siguen fascinándome los inteligentes e innovadores métodos que los delincuentes despliegan para lograr sus objetivos.

Los delincuentes actualizan de manera permanente sus técnicas para incorporar las últimas tecnologías a sus *modi operandi*. Ha llovido mucho desde los tiempos en los que fueron los primeros en usar buscapersonas y utilizar teléfonos móviles de un kilo de peso para enviarse mensajes codificados. Ahora construyen sus propios sistemas de radiotelecomunicaciones móviles encriptadas de alcance nacional[1], como los que emplean los cárteles del narcotráfico en México. Imagina por un instante el grado de sofisticación que se requiere para poner en funcionamiento una red nacional de comunicaciones encriptada operativa, toda una proeza, sobre todo si se tiene en cuenta que muchos estadounidenses aún no reciben una cobertura móvil decente la mayor parte del tiempo.

Las organizaciones ilegales se han consagrado como las principales asimiladoras de las nuevas tecnologías. Los delincuentes utilizaban Internet mucho antes de que la policía ni siquiera contemplara hacerlo, y desde entonces han sacado ventaja a las autoridades. Los titulares de prensa vienen repletos de noticias sobre cuentas online de cien millones de dólares pirateadas por aquí y cincuenta millones de dólares

robados por allá. El avance de estos delitos es alarmante, y siguen acelerando por el mal camino.

El tema de este libro no es qué sucedió en el pasado, ni siquiera qué está sucediendo en el presente. Y tampoco voy a determinar la longitud que debe tener una contraseña. Lo que pretendo es explicar qué nos depara el futuro. Durante mis propias investigaciones, primero con el Departamento de Policía de Los Ángeles y posteriormente colaborando con organismos federales e internacionales que velan por el cumplimento de la ley, he descubierto a delincuentes que han rebasado los ciberdelitos de hoy en día y se han internado en nuevos campos emergentes de la tecnología, como la robótica, la realidad virtual, la inteligencia artificial, la impresión 3D y la biología sintética. En la mayoría de los casos, mis colegas en las esferas gubernamentales y los cuerpos de seguridad desconocen estos avances tecnológicos incipientes, por no mencionar ya su creciente explotación tanto por parte del crimen organizado como de organizaciones terroristas. Y siendo alguien que ha dedicado su vida a la seguridad y el servicio público, me preocupan sobremanera las tendencias que observo a mi alrededor.

Pese a que haya quien me acuse de instigar al miedo o ser un pesimista sin remedio, te aseguro que no soy ninguna de las dos cosas. En realidad, me definiría más bien como un optimista o, mejor dicho, como un «optimista irracional», a tenor de lo que he visto que nos reserva el futuro. Para dejarlo claro de antemano, no soy ningún neoludita, ni tampoco soy tan insensato como para insinuar que la tecnología es el origen de todos los males de nuestra existencia. Muy al contrario: creo en el tremendo poder de la tecnología para ser la fuerza impulsora del bien y soy consciente de que puede emplearse y se ha empleado de múltiples maneras para proteger a personas individuales y a la sociedad en su conjunto. Ahora bien, la tecnología siempre ha sido un arma de doble filo. Mis experiencias en el mundo real con delincuentes y terroristas en seis continentes me han dejado claro que las fuerzas del mal no dudarán en aprovechar estas tecnologías emergentes y desplegarlas contra las masas. Y aunque las evidencias y el instinto me dicen que la carretera que tenemos por delante está llena de baches y que los gobiernos y el sector industrial no dedican suficientes recursos a combatirlos, quiero creer en la tecnoutopía que nos promete Silicon Valley.

Este libro narra la historia de la sociedad que estamos construyendo con las herramientas tecnológicas a nuestro alcance y cómo su implementación puede esgrimirse en nuestra contra. Cuanto más conectamos nuestros dispositivos y nuestras vidas a la redes de información global, ya sea a través de teléfonos móviles, redes sociales, ascensores o coches autodirigidos, más vulnerables nos volvemos frente a quienes saben cómo funcionan las tecnologías subyacentes y cómo explotarlas en beneficio propio y en detrimento del común de los mortales. En pocas palabras, cuando todo está conectado, todo el mundo es vulnerable. La tecnología que aceptamos de manera rutinaria en nuestras vidas, sin cuestionarnos nada ni analizarla,

puede volverse contra nosotros.

Arrojando luz sobre las últimas artes de las organizaciones delictivas y terroristas, pretendo suscitar un debate vibrante y necesario desde hace tiempo entre mis amistades y colegas en los ámbitos de la política y la seguridad nacional. Si bien la mayoría de ellos ya están sobrecargados con los delitos tradicionales, es preciso que antes o después afronten el avance exponencial de las tecnologías, que llegarán a nosotros como un tsunami capaz de desestabilizar la seguridad mundial.

Pero hay algo aún más importante: como alguien que en el pasado juró «proteger y servir» al prójimo, quiero asegurarme de que la población general esté armada con los datos necesarios para protegerse y proteger a sus familias, sus empresas y sus comunidades frente a la horda de amenazas incipientes que serán una realidad mucho antes de lo que anticipamos. Limitar este conocimiento a los iniciados que trabajan para el gobierno, en temas de seguridad o en Silicon Valley, simplemente no basta.

Durante el tiempo que fui funcionario público, colaborando con organismos como el Departamento de Policía de Los Ángeles, el FBI, el servicio secreto estadounidense y la Interpol, cada vez me resultó más obvio que los delincuentes y los terroristas aventajaban a las fuerzas policiales internacionales en cuanto a innovación se refería y que el mundo y los «buenos de la película» cada vez quedaban más rezagados. Con el objetivo de actuar de manera más contundente contra las crecientes legiones de delincuentes que hacen un mal uso de las tecnologías más punteras, dejé el gobierno y me trasladé a Silicon Valley para formarme en qué era lo siguiente que podíamos esperar.

En California me interné en una comunidad de innovadores tecnológicos con vistas a descifrar cómo afectarían sus últimos descubrimientos científicos a las personas de a pie. Visité a los vástagos de Silicon Valley y entablé amistad con la talentosa comunidad de las *start-ups* o empresas noveles de la zona de la bahía de San Francisco. Me invitaron a inscribirme en la facultad de la Singularity University, una institución asombrosa con sede en el campus del Centro de Investigación Ames de la NASA, donde trabajé con un equipo brillante de astronautas, roboticistas, científicos de datos, ingenieros informáticos y biólogos sintéticos. Estos hombres y mujeres pioneros tienen la habilidad de ver más allá del mundo actual y desbloquear el tremendo potencial de la tecnología para salvar los grandes desafíos que afronta la humanidad.

No obstante, muchos de estos emprendedores de Silicon Valley que se esfuerzan con denuedo en crear nuestro futuro tecnológico prestan muy poca atención a los riesgos legales, éticos, de seguridad y para las políticas públicas que sus creaciones entrañan para el resto de la sociedad. En cambio, mi propia experiencia esposando a delincuentes y colaborando con las fuerzas policiales de más de setenta países me obliga a adoptar un planteamiento distinto con respecto a los potenciales usos abusivos de las tecnologías emergentes que las personas inocentes del mundo reciben con alegría en sus vidas cotidianas, generalmente sin cuestionárselo siquiera.

A tal fin, fundé el Future Crimes Institute. Mi cometido era utilizar mis experiencias como agente policial, investigador, analista de contraterrorismo internacional y, más recientemente, persona con información privilegiada de Silicon Valley para catalizar una comunidad de expertos en la materia que aborde tanto las implicaciones negativas como las positivas de unas tecnologías que evolucionan a un ritmo acelerado.

Cuando pienso en el futuro, cada vez me preocupa más la ubicuidad de la informática en nuestras vidas y el hecho de que nuestra total dependencia de ella nos esté haciendo vulnerables de un modo que muy pocos de nosotros somos capaces siquiera de entender. Las actuales interdependencias y complejidades sistémicas son enormes y aumentan sin parar. Sin embargo, existen individuos y grupos que les están hallando sentido e innovan a tiempo real, en detrimento de todos nosotros.

Ésta es su historia, la historia del crimen organizado, de los *hackers* o piratas informáticos, de los gobiernos corruptos, de las entidades subestatales y de los terroristas que compiten por controlar las últimas tecnologías en beneficio propio.

La tecnoutopía prometida por Silicon Valley tal vez sea posible, pero no aparecerá por arte de magia. Será necesario que ciudadanos, gobiernos, empresas y ONG inviertan en ella una dedicación, un esfuerzo y una lucha tremendos para garantizar que llegue a buen puerto. Ha dado comienzo una nueva contienda entre quienes aprovecharán la tecnología en beneficio de la humanidad y quienes prefieren subvertir esas herramientas, al margen del daño que provoquen al prójimo. Estamos ante una batalla por el alma de la tecnología y su futuro. Se propaga en el fondo, de manera encubierta y oculta del ciudadano corriente.

Más allá de catalogar meramente las últimas novedades en innovación criminal y vulnerabilidad técnicas, este libro ofrece un camino para derrotar la miríada de amenazas que nos aguardan. Si somos previsores, creo que es posible anticipar e impedir hoy los delitos del mañana, antes de alcanzar un punto de no retorno. Las generaciones futuras volverán la vista atrás y juzgarán nuestros esfuerzos por domeñar estas amenazas a la seguridad y salvaguardar el alma de la tecnología en pro de garantizar el bien de la humanidad.

Una advertencia amistosa: si continúas leyendo las páginas que siguen, nunca más volverás a ver tu coche, tu teléfono móvil ni tu aspirador del mismo modo.

> Ésta es tu última oportunidad. Después ya no podrás echarte atrás. Si tomas la pastilla azul, fin de la historia. Despertarás en tu cama y creerás lo que quieras creerte. Si tomas la roja, te quedas en el País de las Maravillas y yo te enseñaré dónde llega la madriguera de conejos. Recuerda: lo único que te ofrezco es la verdad. Nada más.
>
> Advertencia de MORFEO a NEO, *Matrix*

PRIMERA PARTE

UNA TORMENTA EN EL HORIZONTE

Capítulo 1

Conectados, dependientes y vulnerables

> La tecnología… es rara: te ofrece grandes regalos con una mano y con la otra te clava una puñalada trapera.
>
> CHARLES PERCY SNOW

La vida de Mat Honan pintaba bien en pantalla: en una pestaña del navegador había imágenes de su hijita recién nacida, mientras que en otra iban apareciendo los tuits de sus miles de seguidores en Twitter. En tanto que periodista de la revista *Wired* en San Francisco, Honan llevaba una vida urbana y conectada y estaba tan al corriente de las últimas tecnologías como cualquiera. Ahora bien, no imaginaba que todo su mundo digital podía borrarse con sólo accionar unas cuantas teclas. Eso fue justamente lo que sucedió un día de agosto. Sus fotografías, su correo electrónico y muchas otras cosas cayeron en manos de un *hacker*. Un adolescente de la otra punta del mundo se lo robó todo en cuestión de minutos. Honan era un objetivo fácil. Todos lo somos.

Honan recuerda la tarde del desastre. Estaba jugando en el suelo con su hijita cuando, de repente, su iPhone se apagó. Pensó que quizá se le había acabado la batería. Esperaba una llamada importante, de manera que conectó el teléfono a la corriente y lo reinició. En lugar de la pantalla de inicio y las aplicaciones habituales, vio un gran logotipo de Apple blanco y una pantalla de bienvenida plurilingüe que lo invitaba a configurar su teléfono nuevo. «¡Qué raro!», se dijo.

Pero no se preocupó demasiado: hacía una copia de seguridad de su iPhone cada noche. El paso siguiente era evidente: conectarse a iCloud y restaurar el teléfono y sus datos. Al iniciar sesión en su cuenta Apple, se le informó de que su contraseña, la que estaba seguro que era correcta, había sido rechazada por los dioses de iCloud. Honan, una sagaz periodista de la revista sobre tecnologías más relevante del mundo, aún guardaba otro as en la manga. Conectaría el iPhone al portátil y restauraría sus datos desde el disco duro de su ordenador de casa. Sin embargo, lo que ocurrió a continuación hizo que se le encogiera el corazón.

Cuando Honan encendió el Mac, le apareció un mensaje del programa de calendario de Apple que le advertía de que su contraseña de Gmail era incorrecta. Inmediatamente después, el rostro de su portátil (es decir, su bonita pantalla) se volvió de color verde ceniza y se apagó, como si hubiera muerto. Lo único visible en la pantalla era una mensaje que decía: «Introduzca su contraseña de cuatro dígitos». Honan sabía que nunca había configurado una contraseña.

Finalmente, Honan descubrió que un *hacker* había tenido acceso a su cuenta de

iCloud y había utilizado la útil función «Buscar mi iPhone» de Apple para localizar todos los dispositivos electrónicos que configuraban el mundo del periodista. Y luego los había destruido uno por uno. El *hacker* activó la orden de «borrado remoto» y, con ella, eliminó todos los datos que Honan había acumulado a lo largo de su vida. El primero en caer fue su iPhone. Lo siguió el iPad. Y, por último, como era de esperar, también sucumbió su MacBook. En un instante, todos sus datos, incluidas las fotos que había tomado del primer año de vida de su hija, quedaron destruidos. Y también desaparecieron los recuerdos fotográficos de valor inestimable de sus parientes difuntos, caídos en el éter a manos de desconocidos.

A continuación, el pirata informático borró la cuenta de Google de Honan. En un pestañeo, ocho años de mensajes de Gmail cuidadosamente seleccionados se habían perdido. Conversaciones laborales, notas, recordatorios y recuerdos eliminados con un solo clic de ratón. Por último, el *hacker* centró su atención en su objetivo final: la cuenta de Twitter de Honan, @Mat. No sólo se apoderó de ella, sino que la utilizó para enviar consignas racistas y homofóbicas en nombre de Honan a sus miles de seguidores.

En la estela de aquel ataque cibernético, Honan empleó sus habilidades como periodista de investigación para reconstruir lo sucedido. Telefoneó al departamento de asistencia técnica de Apple para reclamar su cuenta de iCloud. Tras pasar más de noventa minutos al teléfono, Honan supo que «él mismo» había llamado hacía apenas treinta minutos para solicitar un cambio de contraseña. Resultaba que la única información necesaria para modificar esa contraseña era su dirección de facturación y los últimos cuatro dígitos de su número de tarjeta de crédito. La dirección de Honan aparecía en el registro de dominios de Internet Whois que él mismo había creado al construir su sitio web personal. Pero, aunque no hubiera estado allí, docenas de servicios online, como WhitePages.com y Spokeo, la habrían proporcionado de manera gratuita.

Para conocer los cuatro dígitos de la tarjeta de crédito de Honan, el *hacker* supuso que Honan (como la mayoría de nosotros) tenía una cuenta en Amazon.com. Y acertó. Armado con el nombre completo de Honan y sus direcciones postal y de correo electrónico, contactó con Amazon y logró manipular al empleado del servicio de atención al cliente para obtener acceso a los cuatro últimos dígitos de su tarjeta de crédito. Aquellos sencillos pasos, sin más, pusieron la vida de Honan patas arriba. Y aunque no fue el caso, el *hacker* podría haber utilizado esa misma información para acceder y robar las cuentas bancarias y de corretaje online de Honan.

El adolescente que al final acabó reconociendo el ataque (Phobia, como se lo conocía en los círculos del pirateo informático) alegó que su objetivo era poner de relieve las inmensas vulnerabilidades en la seguridad de los servicios de Internet en los que confiamos cada día. Y quedó bien claro. Honan creó una nueva cuenta de Twitter para comunicarse con su atacante. Desde la cuenta @Mat, Phobia accedió a seguir la nueva cuenta de Honan, cosa que les permitía enviarse mensajes directos el

uno al otro. Honan formuló a Phobia la única pregunta que le hacía hervir la sangre: «¿Por qué? ¿Por qué a mí?». Y resultó que la década de datos y recuerdos perdidos no fue más que un mero daño colateral.

La respuesta de Phobia fue escalofriante: «Sinceramente, no tengo nada en contra de ti… Simplemente me gustó tu nombre de usuario [en Twitter]». Eso era todo. La explicación: un preciado *handle* de tres letras en Twitter. A un *hacker* a miles de kilómetros de distancia le había gustado y había querido adueñarse de él.

La idea de que alguien que no tiene «nada en contra de ti» pueda borrar por completo tu vida digital accionando unas cuantas teclas es inadmisible. Cuando el artículo de Honan fue portada de *Wired* en diciembre de 2012, recibió una atención considerable… durante un par de minutos. Siguió un debate sobre cómo hacer más seguras las tecnologías que usamos a diario, pero, como tantos otros debates en Internet, al final las llamas se consumieron. Y prácticamente nada ha cambiado desde las tribulaciones de Honan. Seguimos siendo tan vulnerables como lo era él entonces, o incluso más, si tenemos en cuenta que hemos incrementado nuestra dependencia de las aplicaciones móviles y basadas en la nube, tan fáciles de piratear.

Como ocurre con la mayoría de nosotros, las diversas cuentas de Honan estaban vinculadas entre sí, en una red autorreferencial de supuesta confianza digital: el mismo número de tarjeta de crédito en el perfil de Apple y en la cuenta de Amazon, y una dirección de correo electrónico en iCloud que remite a Gmail. Todas compartían información como credenciales de acceso y números de tarjeta de crédito y contraseñas, y todos esos datos remitían a una misma persona. Las protecciones en materia de seguridad de Honan eran poco más que una Línea Maginot[*] digital, un castillo de naipes que se desmoronó bajo la menor presión. Toda o prácticamente toda la información necesaria[1] para destruir su vida digital, o en su caso la tuya, está perfectamente disponible online para cualquiera con una mente ligeramente enrevesada o creativa.

Progreso y peligros en un mundo conectado

En apenas unos años, sin reflexionar apenas sobre ello, hemos pasado de utilizar Google meramente para efectuar búsquedas a confiar en él a ciegas para obtener indicaciones de cómo llegar a sitios, guardar nuestros calendarios, agendas, vídeos, mensajes en el buzón de voz y opciones de entretenimiento, e incluso para efectuar llamadas telefónicas. Mil millones de personas hemos publicado nuestros datos más íntimos en Facebook y hemos proporcionado de manera voluntaria gráficos de redes sociales de nuestros amigos, familiares y colegas del trabajo. Nos hemos descargado miles de millones de aplicaciones y las utilizamos para realizar prácticamente todo, desde operaciones bancarias hasta consultar recetas de cocina o guardar fotografías

de nuestros hijos. Nos conectamos a Internet a través de nuestros ordenadores portátiles, teléfonos móviles, iPad, TiVo, televisiones por cable, consolas PS3, Blurays, consolas Nintendo, televisiones de alta definición (HDTV), Rokus, consolas Xbox y Apple TV.

Los aspectos positivos de esta evolución tecnológica son manifiestos. A lo largo de los últimos cien años[2], los rápidos avances registrados por las ciencias médicas han permitido que la esperanza de vida media de los seres humanos se haya más que duplicado y la mortalidad infantil se haya reducido por diez. La renta media por cápita ajustada a la inflación alrededor del mundo se ha triplicado. El acceso a una educación de calidad, que en el pasado estaba reservada a unos privilegiados, es hoy gratuito a través de sitios web como la Khan Academy. Y el teléfono móvil por sí solo es responsable de la generación de miles de millones de dólares en desarrollo económico directo en países de todo el planeta[3].

La interconectividad que proporciona Internet a través de su arquitectura fundamental permite establecer conexiones entre personas dispares de todo el planeta. Una mujer de Chicago puede jugar a *Words with Friends* con un completo desconocido en los Países Bajos. Un médico de Bangalore, India, puede leer e interpretar a distancia los resultados de las radiografías de un paciente en Boca Raton, Florida. Un granjero de Sudáfrica puede utilizar su teléfono móvil para acceder a los mismos datos sobre las cosechas que un doctorando en el Massachusetts Institute of Technology (MIT). Esta interconectividad es uno de los puntos fuertes de Internet y, a medida que se amplía, también lo hace la potencia y la utilidad de la red global. Tenemos muchas cosas que celebrar en el mundo tecnológico actual.

Si bien las ventajas del mundo en línea están bien documentadas y suelen ser destacadas por quienes trabajan en el sector de las tecnologías, toda esta interconectividad también tiene un lado oscuro.

Los tendidos eléctricos, el control del tráfico aéreo, los sistemas de envío de camiones de bomberos e incluso los ascensores de nuestros lugares de trabajo dependen esencialmente de la informática. Cada día conectamos más parte de nuestras vidas cotidianas a la red de información global sin detenernos a pensar qué implicaciones tiene ello. Mat Honan lo descubrió por las malas aquel día, tal como les ha ocurrido a miles de personas. Pero ¿qué sucedería si todas las instalaciones tecnológicas de la sociedad moderna, es decir: las herramientas fundacionales de las cuales dependemos por completo, desaparecieran? ¿Cuál es el plan B de la humanidad? No existe.

El mundo es plano (y está abierto de par en par)

Durante siglos, el sistema de Westfalia de los Estados nación soberanos ha

prevalecido en el mundo[4]. Dicho sistema implicaba que los países eran soberanos en su territorio y las autoridades foráneas no podían intervenir en sus asuntos interiores. La estructura de Westfalia se preservaba mediante un sistema de fronteras, ejércitos, guardias, barreras y armas. Podían implantarse controles para limitar los movimientos migratorios de personas en un territorio nacional. Más aún, se establecían aduanas y estructuras de inspección para controlar el paso de bienes a través de las fronteras nacionales. Sin embargo, por muy clarividentes que fueran los signatarios del Tratado de Westfalia en 1648, ninguno de ellos barruntó la existencia de Snapchat[*].

Si bien las fronteras físicas continúan teniendo un papel relevante, tales divisiones son mucho menos claras en el mundo virtual. Los bits y *bytes* fluyen libremente de un país a otro sin someterse a controles fronterizos, controles de inmigración o declaraciones de aduanas que ralenticen su tránsito. Las barreras transnacionales tradicionales a la delincuencia que debían superar las generaciones anteriores de ladrones, mafiosos y convictos se han demolido en el mundo virtual y han permitido que individuos desagradables entren y salgan a su antojo de cualquier sitio web que les plazca.

Piensa en las implicaciones que ello tiene para nuestra seguridad. En el pasado, si un atracador intentaba robar un banco en la neoyorquina plaza Times Square, varios aspectos se habrían dado por sentados. En primer lugar, los atracadores habrían entrado en un lugar físico enmarcado en las fronteras del distrito policial del barrio de Midtown South, correspondiente al Departamento de Policía de Nueva York (NYPD). En segundo lugar, el atraco al banco habría quebrantado tanto las leyes federales de Estados Unidos como la legislación del estado de Nueva York, y el NYPD y el FBI compartirían la jurisdicción para investigar lo sucedido. La víctima (en este caso, el banco) también habría pertenecido a la jurisdicción física de las autoridades garantes del cumplimiento de la ley implicadas, lo cual habría simplificado sobremanera la investigación. Los intentos de resolver el caso se habrían visto apuntalados por las pruebas físicas que el atracador seguramente habría dejado en la escena del crimen, como las huellas dactilares en un billete entregado a un cajero o los restos de ADN en el mostrador sobre el cual saltó, y quizá también a través de las imágenes de su propio rostro grabadas por el sistema de cámaras de seguridad del banco. Además, para cometer el delito el atracador habría tenido que afrontar una serie de limitaciones físicas. Los billetes de dólares robados tendrían volumen y peso y sólo habría sido podido llevarse una cantidad limitada. Y las pilas de efectivo tal vez habrían incorporado un paquete de tinta explosiva que permitiría a la policía seguir el rastro al sospechoso. En cambio, en el mundo actual, todas estas asunciones en materia de investigación establecidas por tradición y de eficacia contrastada, como la jurisdicción compartida y las pruebas físicas, herramientas fundamentales para ayudar a las autoridades a resolver delitos, han dejado de existir.

Compara el escenario del atraco en Times Square que acabamos de describir con el tristemente famoso atraco a un banco por Internet perpetrado en 1994 por Vladimir

Levin desde su piso en San Petersburgo, Rusia. Levin, un programador informático, fue acusado de acceder ilegalmente a las cuentas de varios clientes empresariales importantes de Citibank y sustraerles 10,7 millones de dólares[5]. En colaboración con varios cómplices repartidos por el planeta, Levin transfirió grandes sumas de efectivo a cuentas en Finlandia, Estados Unidos, los Países Bajos, Alemania e Israel.

¿A quién correspondía la jurisdicción de este delito? ¿A la policía de Estados Unidos, donde se ubicaba la víctima (Citibank)? ¿O a la policía de San Petersburgo, desde donde el sospechoso perpetró el supuesto delito? ¿O tal vez la jurisdicción recaía en Israel o Finlandia, donde los bienes ilícitos se ingresaron electrónicamente en cuentas fraudulentas? Levin no puso los pies en Estados Unidos para cometer el delito. No dejó huellas dactilares ni restos de ADN ni quedó marcado por un paquete explosivo de tinta. Y lo más importante, no necesitó sacar físicamente los miles de kilos de dinero del banco, sino que realizó toda aquella operación con un ratón y un teclado. No le hicieron falta ni un pasamontañas ni un arma recortada; le bastó con esconderse tras la pantalla de su ordenador y utilizar una ruta virtual enrevesada para borrar sus huellas digitales.

La esencia misma de Internet implica que vivimos en un mundo sin fronteras. Hoy en día, cualquiera, con buenas o malas intenciones, puede viajar virtualmente a la velocidad de la luz a la otra punta del planeta. Para los delincuentes, esta tecnología ha sido una bendición, pues saltan de un país al otro y desdibujan virtualmente sus desplazamientos por el mundo con vistas a frustrar a la policía. Además, los delincuentes han aprendido a protegerse para que no les sigan el rastro por Internet. Un *hacker* inteligente nunca iniciaría directamente un atraco a un banco en Brasil desde su propia vivienda en Francia. En su lugar, iría encadenando su ataque de red en red, de Francia a Turquía y luego a Arabia Saudí hasta llegar a su objetivo final en Brasil. Esta posibilidad de saltar entre países, uno de los puntos fuertes de Internet, crea enormes problemas jurisdiccionales y administrativos a la policía y es uno de los motivos fundamentales por los cuales la investigación de ciberdelitos supone un desafío de tal magnitud y a menudo no es inútil. Un agente de policía de París no tiene autoridad para efectuar un arresto en São Paulo.

Los buenos tiempos de los ciberdelitos

La naturaleza de las amenazas cibernéticas ha cambiado de manera espectacular en el transcurso de los últimos veinticinco años. En el amanecer de los ordenadores personales, a los piratas informáticos les motivaba, principalmente, «echarse unas risas». Pirateaban sistemas informáticos sólo para demostrar que podían hacerlo. Uno de los primerísimos virus informáticos que infectó los PC de IBM fue el virus Brain[6], creado en 1986 por los hermanos Amjad y Basit Farooq Alvi, de

veinticuatro y diecisiete años de edad respectivamente, residentes en Lahore, Pakistán. Su virus pretendía ser inocuo: detener a otros de piratear el *software* que aquellos dos hermanos habían invertido años en desarrollar. Brain funcionaba infectando el sector de arranque de un disquete como medio de evitar que fuera copiado, y permitía a los hermanos rastrear las copias ilegales de su programa. Los hermanos, enfadados por el hecho de que hubiera quien estuviera copiando su programa informático sin pagar por él, incluían un mensaje de advertencia que aparecía en las pantallas de los usuarios infectados:

Bienvenido a las Mazmorras © 1986 Brain & Amjads (privado).
BRAIN COMPUTER SERVICES 730 NIZAM BLOCK
ALLAMA IQBAL LAHORE, PAKISTÁN.
TELÉFONOS: 430791, 443248, 280530. Tienes un VIRUS…
Si quieres la vacuna, contacta con nosotros…

Su mensaje es destacable por diversos motivos. En primer lugar, los hermanos afirmaban ser los propietarios de los derechos de *copyright* de su virus, un gesto de armas tomar, cuando menos. Y más extraño aún era que incluyeran su dirección postal y números telefónicos para que los usuarios contactaran con ellos con el fin de «vacunarse» o eliminar el virus. Basit y Amjad consideraron que su motivación para crear el virus era lógica, pero no se les ocurrió que su creación tenía la capacidad de replicarse y difundirse, y que lo hizo a la antigua usanza, mediante seres humanos que trasportaban disquetes de 5,25 pulgadas de ordenador en ordenador. Al final, Brain viajó por todo el planeta y presentó a Basit y Amjad al resto del mundo[7].

Con el tiempo, los piratas informáticos se volvieron más ambiciosos… y más malvados. El hecho de estar interconectados mediante servicios de sistemas de boletines de anuncios informáticos implicaba que los virus digitales ya no necesitaban viajar a través de una *sneakernet*, es decir: transportados por una red en la que los propios humanos pasaban la información físicamente mediante disquetes, sino que podían propagarse vía módem a través de las líneas telefónicas mediante los primeros servicios de Internet que existieron, como CompuServe, Prodigy, EarthLink y AOL. Virus más nuevos y troyanos como Melissa (1999), ILOVEYOU (2000), Code Red (2001), Slammer (2003) y Sasser (2004) podían infectar ahora con suma facilidad ordenadores de todo el mundo que tuvieran un sistema operativo Microsoft Windows, destruyendo a su paso exámenes trimestrales, recetas, cartas de amor y hojas de cálculo empresariales guardadas en discos duros. De repente, cualquiera era vulnerable.

El *malware* o *software* dañino, un compuesto formado por las palabras «*mal*icioso» y «soft*ware*», hoy adopta múltiples formas, pero su objetivo es invariablemente dañar, interrumpir, robar o perpetrar alguna acción ilegítima o no autorizada en una red o un sistema de datos:

- Los virus informáticos se propagan insertando una copia de sí mismos en otro programa, tal como los virus del mundo real infectan a un huésped biológico disponible.
- Los gusanos informáticos también provocan daños, pero lo hacen a modo de *software* independiente y no precisan de un programa huésped para replicarse.
- Los troyanos, así bautizados en honor al mítico caballo de madera que los griegos utilizaron para infiltrarse en Troya, suelen camuflarse bajo fragmentos legítimos de *software* y se activan cuando se engaña al usuario para que cargue o ejecute los archivos de un sistema seleccionado. Los troyanos suelen crear «puertas traseras» que permiten a los *hackers* poder acceder siempre que quieran al sistema infectado. Los troyanos no se reproducen infectando otros archivos en sí, sino que se propagan engatusando a los usuarios para que hagan clic en un archivo o abran un fichero adjunto a un correo electrónico infectado.

Los programadores de virus de hoy en día reconocen que el público ha empezado a entender (aunque muy despacio) que no tiene que hacer clic en archivos enviados por desconocidos. Como resultado de ello, los delincuentes han actualizado sus tácticas y han concebido las llamadas «descargas no autorizadas», que utilizan *malware* para aprovechar las vulnerabilidades de los lenguajes de programación con *scripts* como Java y ActiveX, comúnmente utilizados por los navegadores web. El mundo ha pasado a estar conectado en línea, y piratear herramientas como Internet Explorer, Firefox y Safari tiene todo el sentido para los delincuentes, pese a que el nuevo *modus operandi* se salde con un alto precio para los usuarios desprevenidos. Los investigadores de Palo Alto Networks descubrieron que en torno al 90 por ciento del *malware* actual se propaga a través de sitios web populares previamente pirateados que infectan el ordenador en el momento en el que un visitante desprevenido los visita[8]. Muchas grandes empresas, incluida Yahoo!, un importante portal mundial, han visto cómo sus sitios web eran secuestrados por delincuentes y han envenenado sin saberlo a sus propios clientes, quienes, inocentes, acudían a ellos para comprobar resultados de deportes o los últimos movimientos bursátiles[9].

La explosión del *software* malicioso

Ahora los piratas informáticos ya no buscan sólo «echarse unas risas», sino que actúan para conseguir dinero, información y poder. A principios del siglo XXI, a medida que los delincuentes imaginaban nuevos modos de monetizar su *software* malicioso mediante suplantación de identidad y otras técnicas, el número de virus se disparó. En 2015, el volumen era ya asombroso. En 2010, el instituto de investigación

alemán AV-Test había evaluado que existían unos cuarenta y nueve millones de vetas de *software* malicioso en la jungla[10]. En 2011, la empresa de antivirus McAfee informó de que estaba identificando dos millones de programas de *malware* nuevos cada mes. En verano de 2013, la empresa de ciberseguridad Kaspersky Lab anunció que estaba identificando y aislando cerca de 200 000 nuevas muestras de *software* malicioso al día[11].

Si interpretamos estas estadísticas con «ojo cínico» y partimos de la base de que a las empresas de antivirus puede interesarles exagerar el problema que combaten, podríamos desinflar esas cifras de manera espectacular, pongamos por caso en un 50 o incluso un 75 por ciento. Aún así, eso implicaría que cada día se generan cincuenta mil nuevos virus. Piensa en el tremendo esfuerzo en investigación y desarrollo que se precisaría a nivel mundial para crear ese volumen de *software* malicioso con código exclusivo.

Como sabe cualquier empresario, la I+D es cara. Es decir, que la rentabilidad de las inversiones (ROI) requerida para financiar los esfuerzos de programación informática ilegales que realiza de manera continuada el crimen organizado internacional tienen que ser ingentes. Un estudio independiente efectuado por la avalada Consumers Union, editora de la revista *Consumer Reports*, parece confirmar el impacto creciente del *malware* informático. Un sondeo realizado entre sus miembros reveló que un tercio de los hogares estadounidenses había experimentado una infección con *software* malicioso en el año previo, lo cual había costado a los consumidores la gigantesca suma de 2300 millones de dólares al año[12]. Y eso sólo contando a las personas que se dan cuenta de que les han atacado.

La seguridad ilusoria

Cada año, clientes y empresas de todo el mundo depositan su fe en la industria del *software* de seguridad informática para que los protejan de la amenaza creciente del *software* malicioso. De acuerdo con un estudio acometido por el grupo Gartner, el gasto mundial en *software* de seguridad rondaba los 20 000 millones de dólares en 2012 y la previsión es que ascienda vertiginosamente hasta los 94 000 millones de dólares anuales invertidos en ciberseguridad en 2017[13].

Si se pregunta al ciudadano de a pie cómo combatir los virus informáticos, su primera respuesta será utilizando un producto antivirus de una empresa como Symantec, McAfee o Trend Micro. Es una respuesta instintiva procedente de un público a quien se ha entrenado bien. Mas, pese a que estas herramientas pueden haber demostrado su utilidad en el pasado, están perdiendo eficacia a un ritmo acelerado, y las estadísticas son más que reveladoras. En diciembre de 2012,

Researchers at Imperva, una empresa de seguridad de datos con sede en Redwood Shores, California, y los alumnos del Technion-Israel Institute of Technology decidieron comprobar las herramientas antivirus estándar. Recopilaron ochenta y dos nuevos virus informáticos y sometieron aquellos programas de *software* maliciosos a los motores de detección de amenazas de más de cuarenta de las principales empresas de antivirus del mundo, incluidas entre ellas Microsoft, Symantec, McAfee y Kaspersky Lab. El resultado: la tasa de detección de amenazas inicial fue de sólo un cinco por ciento, lo cual implicaba que el 95 por ciento del *malware* pasaba completamente desapercibido[14]. Y también significa que el *software* de antivirus que ejecutas en tu ordenador probablemente sólo evite el cinco por ciento de las amenazas contra tu máquina. Si el sistema inmunitario de tu cuerpo tuviera un promedio de bateo así, habrías muerto en cuestión de horas.

Meses después, los mastodontes del sector del *software* de seguridad actualizan sus programas, pero, lógicamente, suele ser demasiado tarde. El meollo de la cuestión es que los delincuentes y los programadores de virus sacan una enorme ventaja en materia de innovación y astucia a la industria de los antivirus establecida para protegernos frente a estas amenazas. Peor aún, la «tasa de tiempo para la detección» o, lo que es lo mismo, el tiempo que se tarda desde que se lanza un *software* malicioso «al ancho mundo» hasta que es descubierto, está aumentando. Por ejemplo, en 2012, los investigadores del Kaspersky Lab de Moscú descubrieron un *malware* sumamente complejo bautizado como Flame que había estado hurtando datos de los sistemas de información de todo el mundo durante más de cinco años antes de ser detectado. Mikko Hypponen, el respetado agente al frente de la investigación en la empresa de seguridad informática F-Secure, afirmó que Flame era un fracaso de la industria de los antivirus y destacó que él y sus colegas podían haber quedado «desclasificados de sus ligas en su propio juego». Pese a que millones de personas en todo el mundo confían en estas herramientas, está bastante claro que la era de los antivirus ha tocado su fin[15].

Uno de los motivos que explican que esté resultando tan difícil contrarrestar la amplia variedad de amenazas tecnológicas que asedian nuestras vidas cotidianas es la expansión de los llamados «ataques de día cero». Un ataque de día cero aprovecha una vulnerabilidad previamente desconocida de una aplicación informática antes de que los programadores y el personal de seguridad tengan tiempo para subsanarla. En lugar de buscar de manera proactiva estas vulnerabilidades por cuenta propia, las empresas de *software* antivirus sólo analizan puntos de referencia conocidos. Así, bloquearán un fragmento de código malicioso si es igual que otro fragmento de código malicioso que hayan detectado previamente. En esencia, sería como colgar un cartel de «Se busca a Bonnie y Clyde» porque sabemos que han robado bancos en el pasado. Los cajeros de banco sabrían que tenían que estar al tanto por si identificaban a la pareja, pero, mientras no se materializara nadie que encajara con su descripción, podían tener la guardia baja… hasta que apareciera otro atracador. Cada vez se

generan más «días cero» para una amplia gama de productos tecnológicos que usamos de manera habitual en nuestras vidas y que afectan a cualquier cosa, desde el sistema operativo Microsoft Windows hasta *routers* Linksys o los omnipresentes programas PDF Reader o *Flash* Player de Adobe.

Con el tiempo, los *hackers* se dieron cuenta de que, cuanto más ruido hicieran al colarse en nuestros sistemas, más rápidamente solucionaríamos el problema y los expulsaríamos. Así que ahora lo que impera es el sigilo y la clandestinidad, como si tuviéramos una célula durmiente en el ordenador. Tal vez pienses que la pésima tasa de detección de virus informáticos del cinco por ciento revelada por el estudio Imperva se aplicaba exclusivamente a los ciudadanos medios que utilizan *software* de seguridad personal en sus hogares. Es imposible que las empresas, con el monumental presupuesto que invierten en tecnologías de la información y seguridad, sean tan vulnerables ante los *hackers*, ¿no es cierto? Pues te equivocas. Decenas de miles de ataques con éxito perpetrados contra grandes empresas, ONG y gobiernos de todo el mundo revelan que, pese al capital que invierten, no consiguen proteger su información mucho mejor que el común de los mortales.

De acuerdo con el *2013 Data Breach Investigations Report* de Verizon, la mayoría de las empresas han demostrado ser simple y llanamente incapaces de detectar cuándo un *hacker* se infiltra en sus sistemas de información. Esta emblemática encuesta realizada por los servicios empresariales de Verizon en colaboración con los servicios secretos de Estados Unidos, la Policía Nacional holandesa y la Unidad de Delitos Cibernéticos de la Policía del Reino Unido, informó de que un promedio del 62 por ciento de las intrusiones contra empresas tardaba aproximadamente dos meses en detectarse[16]. Un estudio similar de Trustwave Holdings revelaba que el tiempo promedio desde la infiltración inicial en la red de una empresa hasta la detección de tal intrusión era de 210 días[17]. Alarmante, ¿no es cierto? Son casi siete meses para que el atacante, ya se trate de una mafia, de la competencia o de un gobierno extranjero, merodee a sus anchas por una red corporativa robando secretos, aprovechando los conocimientos de la competencia, infiltrándose en sistemas financieros y hurtando datos personales identificativos de los clientes, como los números de sus tarjetas de crédito.

Y cuando finalmente las empresas se dan cuenta de que tienen un espía digital en su seno y de que sus sistemas de información vitales han quedado expuestos, un lamentable 92 por ciento de las veces no es el gerente de TI de la empresa ni el equipo encargado de la seguridad ni el administrador del sistema quien descubre la infracción[18]. Normalmente, los cuerpos de seguridad, un cliente enfadado o un contratista notifican el problema a la víctima. Si los *hackers* son capaces de penetrar tan fácilmente en las mayores corporaciones mundiales, empresas que de manera colectiva invierten millones en ciberdefensa y cuentan con departamentos exclusivos de profesionales que trabajan las veinticuatro horas del día de los siete días de la semana para proteger sus redes, las perspectivas de que los usuarios domésticos

protejan su información se antojan como mínimo agoreras.

¿Cuánto cuesta infiltrarse en un sistema informático normal? Es tan fácil que da risa. Según el estudio de Verizon, una vez que los *hackers* ponen la vista en la red de alguien, en el 75 por ciento de las ocasiones son capaces de penetrar sus defensas en cuestión de minutos. El mismo estudio apunta que sólo el 15 por ciento de las veces tardan más de unas cuantas horas en franquear un sistema. Las implicaciones de estos hallazgos son profundas. Desde el momento en que un atacante decide atacar el mundo de alguien, el 75 por ciento de las veces consigue hacerlo en pocos minutos[19]. Y la víctima recibe el impacto y cae derribada al suelo antes de saber siquiera quién o con qué le ha golpeado. En el mundo actual, los *hackers* campan a sus anchas por las entrañas de nuestros sistemas de datos durante meses y meses, observándonos, esperando, acechando y saqueándolo todo, desde nuestras contraseñas hasta proyectos laborales y autorretratos del pasado. Somos presas fáciles, dianas perfectas. Y es extraño que, en tanto que sociedad, toleremos que esto suceda. Si alguno de nosotros descubriera a un ladrón en nuestro hogar observándonos mientras dormimos o filmándonos en la ducha, llamaría inmediatamente a la policía (o gritaría o iría en busca de un arma). En el ciberespacio, esto sucede a diario y, sin embargo, la mayoría seguimos tan panchos, felizmente ajenos a la amenaza, pese a nuestras profundas vulnerabilidades y a que los malos se ciernen sobre nosotros mientras dormimos.

El coste de nuestra ciberinseguridad continúa ascendiendo. Si bien la inversión de las empresas mundiales en todo un abanico de medidas de seguridad para *software* y *hardware* rondará los cien mil millones en 2017, esa cifra no es más que un punto de partida a la hora de considerar el impacto económico total de nuestra fragilidad tecnológica. Pongamos por ejemplo la ciberhuelga que se convocó en 2007 contra TJX, la empresa madre de las tiendas al por menor T. J. Maxx y Marshalls en Estados Unidos y T. K. Maxx en Europa.

En aquel caso, los *hackers* robaron los datos de las tarjetas de crédito de más de cuarenta y cinco millones de clientes, lo cual lo convirtió en el caso de pirateo informático de tiendas minoristas más sonado de su época[20]. En los documentos presentados posteriormente ante los tribunales se reveló que el número real de víctimas rozaba los noventa y cuatro millones[21]. Pese a que TJX alcanzó un acuerdo con Visa, MasterCard y sus clientes por la cantidad de 256 millones de dólares, muchos analistas creen que los costes reales podrían haber ascendido fácilmente a los mil millones de dólares[22]. Una de las fuentes más fiables en materia del coste del hurto de datos es el Ponemon Institute, que lleva a cabo investigaciones independientes acerca de protección de datos y políticas de seguridad de la información[23]. A la hora de calcular infracciones a la seguridad en el ciberespacio, el Ponemon Institute recalca que es importante extender el análisis de las pérdidas bastante más allá de las cantidades sustraídas a los clientes directos.

Por ejemplo, la empresa víctima de los ataques, en este caso TJX, debe hacer una

inversión cuantiosa en detectar la infracción, contener a los atacantes, investigar el asunto, identificar a los perpetradores y reparar y recuperar su red informática. Además, suelen producirse graves caídas de ventas, pues el público, receloso, tiene miedo de utilizar los servicios de una empresa que se percibe como insegura. Súmese a ello el precio de las tasas de sustitución de las tarjetas de crédito (que actualmente rondan los 5,10 dólares por tarjeta), los servicios de monitorización del crédito de los clientes que debe adquirir la empresa víctima para impedir nuevos fraudes contra sus clientes con las tarjetas de créditos y las primas cada vez más cuantiosas de los ciberseguros, y uno se da cuenta enseguida de la rapidez con la que dichas pérdidas ascienden[24]. De ahí que muchas empresas rehúsen admitir que las han pirateado y otras intenten negar la infracción durante el máximo tiempo posible.

Hay otros costes adicionales, más graves, a tener cuenta, incluido cómo los mercados bursátiles castigan a las empresas víctimas con desplomes precipitados en el precio de sus acciones tras un ciberataque. En una ocasión, Global Payments vio cómo su valoración en el mercado se recortaba en un nueve por ciento en sólo un día hasta que finalmente la Bolsa de Nueva York dejó de vender sus acciones[25]. Además de los quebraderos de cabeza económicos que entrañan estos casos, están las demandas colectivas subsiguientes de los clientes, accionistas y reguladores de la empresa. Dicho esto, el Ponemon Institute calcula que las empresas afrontan unos costes de 188 dólares por cada registro robado. Multiplíquese esa cantidad por los cerca de cien millones de registros de cuentas de TJX y enseguida se obtendrá una idea de cómo crecen exponencialmente los costes de estas infracciones[26].

En total, entre las sumas gastadas en medidas de prevención (en su mayoría ineficaces) y en cerrar retroactivamente las puertas del ciberestablo después de que salgan los caballos (y entren los *hackers*), en tanto que sociedad pagamos muy cara nuestra inseguridad tecnológica. Y lo que es aún peor, nuestra creciente conexión al mundo virtual y nuestra radical dependencia concomitante de tecnologías completamente penetrables pueden hacernos mucho más daño del que entrañan para nuestros bolsillos colectivos.

Internet ha perdido su inocencia. Nuestro mundo interconectado se está volviendo un lugar cada vez más peligroso y cuantas más tecnologías expugnables incorporemos a nuestras vidas, más vulnerables nos volveremos. La próxima Revolución industrial, la revolución de la información, está en marcha, con consecuencias a gran escala aún imprevistas para nuestra seguridad personal y global. Mas, por abrumadoras que se antojen estas amenazas para las personas, organizaciones e incluso para nuestras infraestructuras vitales hoy en día, hay un tren tecnológico proverbial que ya ha salido de la estación y acelera de manera exponencial. Hay indicios de ello por todas partes, detectables por cualquiera que sepa dónde buscar.

En el horizonte se perfilan nuevas tecnologías, incluidas la robótica, la inteligencia artificial, la genética, la biología sintética, la nanotecnología, la

fabricación en 3D, la ciencia del cerebro y la realidad virtual, todas las cuales tendrán repercusiones de gran calado en nuestro mundo y plantearán una panoplia de amenazas a la seguridad que harán que los ciberdelitos habituales de hoy en día parezcan un juego de niños. Estas innovaciones desempeñarán papeles esenciales en nuestras vidas diarias en cuestión de pocos años y, pese a ello, todavía no se ha realizado ningún estudio abarcador en profundidad que nos ayude a entender los riesgos colaterales que plantean.

La profundidad y el alcance de esta transformación y de sus riesgos concomitantes suelen pasar desapercibidos a la mayoría de las personas, pero, antes de que nos demos cuentas, en nuestra sociedad global habrá conectados a Internet tres mil billones de dispositivos nuevos, dispositivos que permearán cada aspecto de nuestras vidas. Estas conexiones permanentes nos vincularán a hombres y máquinas a lo ancho y largo del planeta, para bien y para mal, y se entretejerán en el fondo de nuestra conciencia común, donde se expandirán de manera exponencial. Como resultado de ello, la tecnología ya no girará sólo en torno a las máquinas, sino que se convertirá en la historia de la vida en sí. Quienes sepan cómo funcionan estas tecnologías subyacentes estarán cada vez mejor posicionados para explotarlas en su beneficio y, como hemos visto, en detrimento de los ciudadanos corrientes. La cornucopia de tecnología a la que hemos dado cabida en nuestras vidas, con poca o nula reflexión ni examen a conciencia, puede volverse en nuestra contra. Estos riesgos presagian la nueva normalidad, un futuro para el cual no estamos preparados en absoluto. Este libro versa acerca de los hombres y las máquinas y acerca de cómo los esclavos pueden convertirse en los amos.

Capítulo 2

Sistema fallido

> Si continuamos desarrollando tecnología sin sabiduría o prudencia, es posible que nuestro siervo acabe convirtiéndose en nuestro ejecutor.
>
> OMAR N. BRADLEY

Tenía que haber algún error en las señales[1]. Era un martes de principios de enero de 2008 cuando un tranvía en Lodz, Polonia, giró de manera brusca y repentina hacia la izquierda. Eso, en sí, no era tan raro, salvo por el hecho de que el maquinista había intentado hacerlo girar hacia la derecha. Instantes después, los vagones traseros descarrilaron y chocaron con otro tranvía antes de detenerse entre chirridos.

Asombrosamente, a juzgar por la magnitud de la colisión, no se produjeron víctimas mortales, pero más de una docena de pasajeros resultaron heridos y muchos otros se rascaban la cabeza, sin entender nada. ¿Qué había sucedido? En lugar de un fallo en los circuitos o un error humano por parte del maquinista, los ingenieros ferroviarios no tardaron en sospechar que se trataba de un sabotaje. Y estaban en lo cierto, pero por razones que probablemente nunca habrían contemplado.

Resultó que un cerebrito de la informática de catorce años había creado un transmisor remoto por infrarrojos capaz de controlar todos los cruces del sistema de tráfico. El chaval se había pasado meses estudiando el sistema ferroviario de la ciudad con vistas a determinar los mejores lugares para desviar los trenes y provocar el máximo caos, y para ello pirateó los interruptores de toda la ciudad para redirigir los trenes a su antojo[2].

En otras palabras, el adolescente consiguió utilizar el sistema de tranvías urbano como su «tren de juguete personal» pirateando y manejando electrónicamente la infraestructura del tráfico urbano[3]. Se creía que el muchacho había utilizado el dispositivo en numerosas ocasiones y cuando fue arrestado, admitió, como el *hacker* de Mat Honan, que lo había hecho «sólo por divertirse».

Pero su broma conllevó el descarrilamiento de cuatro tranvías y podría haber causado víctimas mortales, una diferencia importante que hizo que los analistas de seguridad se enfurecieran por el hecho de que no se estuvieran tomando medidas adicionales para garantizar la seguridad de las infraestructuras básicas de la ciudad. Con razón argumentaron que si un chaval de catorce años que actuaba por cuenta propia podía piratear la red del sistema de tráfico y ocasionar aquel caos por mera diversión, ¿qué iba a impedir que los delincuentes, terroristas o un país enemigo hicieran exactamente lo mismo?

Un panel de información global vulnerable

Hemos visto lo fácil que es piratear la mayoría de los sistemas informáticos y la rapidez con que puede hacerse. La experiencia de Mat Honan demostró que nuestras vidas digitales pueden borrarse en un abrir y cerrar de ojos. T. J. Maxx y Citibank descubrieron por las malas qué puede suceder cuando delincuentes a miles de kilómetros de distancia te sitúan en su punto de mira. A tenor de los peligros más evidentes, cualquiera pensaría que se adoptarían medidas prudentes antes de añadir nada que se conecte a una toma de corriente de pared o use una batería para acceder a la red de información global y, sin embargo, continuamos avanzando a toda máquina en nuestro idilio creciente con todo lo tecnológico.

Como resultado, cada vez estamos más conectados a sistemas informáticos de modos que escapan a nuestra comprensión. Estas conexiones son por completo vulnerables y no merecen confianza alguna, unos cimientos bastante frágiles sobre los cuales construir la sociedad de la información del siglo XXI. Y, sin embargo, eso es lo que estamos haciendo. No sólo nuestros ordenadores personales o laborales están íntimamente enredados en Internet, sino que también lo están todas las infraestructuras esenciales de las cuales depende la sociedad moderna. El tendido eléctrico, los gasoductos, los sistemas de emergencias, el control del tráfico aéreo, el mercado bursátil, el agua potable, el alumbrado público, los hospitales y los sistemas de saneamiento y salud pública dependen de tecnologías y de Internet para funcionar. En este mundo nuevo, hemos sacado al ser humano del organismo y hemos convertido a las máquinas en la médula ósea de la civilización.

Las transacciones con tarjeta de crédito, las terminales de pago en los puntos de venta y los cajeros automáticos que mantienen el flujo mundial de comercio y capitalismo zumbando se frenarían en seco sin los ordenadores que ejecutan la red. Los ordenadores deciden cómo, hacia dónde y cuándo encaminar la electricidad para garantizar la estabilidad del tendido eléctrico. Y sistemas de distribución asistidos por ordenadores llevan un registro de los coches patrulla, ambulancias y camiones de bomberos para que quienes deben enviarlos sepan quién está disponible y más cerca para responder en caso de emergencia. Para asomarse a cómo podría ser este mundo distópico sin ordenadores ni electricidad, basta con encender el televisor y darse un baño de apocalipsis en clave tecno y zombis con series como *The Walking Dead* o visionar alguna película del estilo de *El planeta de los simios* o *La jungla 4.0*. Maquinaciones de Hollywood aparte, nuestras infraestructuras informativas fundamentales basadas en la informática cada vez se ven sometidas a más ataques y son profundamente vulnerables a un fallo sistémico cuyo impacto podría acarrear una catástrofe sin precedentes.

La mayoría de las infraestructuras básicas del mundo utilizan sistemas de supervisión, control y adquisición de datos SCADA (acrónimo de Supervisory

Control and Data Acquisition) para funcionar. Los sistemas SCADA «supervisan y ajustan de manera automática la activación, producción y otras actividades de control de proceso en función de los datos de retroalimentación digitalizados recogidos por sensores»[4]. Se trata de sistemas informáticos especializados, en su mayoría anticuados, que controlan equipamiento físico con funciones tan dispares como hacer circular los trenes por las vías y distribuir la energía en una ciudad. De manera creciente, los sistemas SCADA se están conectando a la Internet más amplia, lo cual tiene implicaciones destacables para la seguridad de todos. Por desgracia, estos sistemas no se diseñaron teniendo en mente la seguridad y su ingeniería no se concibió para que fueran resistentes a un mundo conectado a la Red. Pero el problema es más grave de lo que podría pensarse: en un estudio sobre empresas de infraestructuras básicas de varios sectores efectuado en julio de 2014 se descubrió que cerca del 70 por ciento de ellas había sufrido al menos una brecha en la seguridad que había conllevado la pérdida de información confidencial o la interrupción de las actividades durante los doce meses previos[5].

¿Qué podría hacer un *hacker* con acceso a estos sistemas? Pensemos, por ejemplo, en los complejos sistemas de tecnologías de la información que regulan las instalaciones de tratamiento de aguas municipales. El sistema SCADA mide de manera constante y ajusta la mezcla apropiada de sustancias químicas para depurar nuestras aguas y potabilizarlas para su consumo. ¿Qué pasaría si se pirateara un sistema así? ¿Podría verterse una mezcla con la cantidad incorrecta de sustancias químicas y, en lugar de purificar el agua, envenenarla? Podría sonar a fantasía, pero ya se ha dado un caso en el que unos piratas informáticos perpetraron un ataque contra el Departamento de Agua y Alcantarillado de South Houston, Texas, según un informe de la BBC datado de 2011[6]. La dirección del protocolo de Internet del atacante remitía a Rusia y se dice que los *hackers* involucrados se dedicaron a encender y apagar repetidamente una bomba hasta que dejó de funcionar. Y si bien nadie enfermó a consecuencia de aquel ataque, la prueba de concepto quedó demostrada.

¿Qué otros ataques a las infraestructuras podrían darse? Pues resulta que el cielo es el límite, como descubrió la torre de control de la Administración Federal de Aviación de Worcester, Massachusetts, ya en 1998. Un adolescente lugareño utilizó sus conocimientos en informática para interrumpir las comunicaciones entre un avión que debía realizar un aterrizaje y la torre de control, e incluso apagó las luces de la pista donde debía aterrizar[7]. Y si bien el incidente no provocó víctimas mortales, el potencial para el desastre que podría haber ocasionado salta a la vista. Por supuesto, se han producido más ataques contra infraestructuras de información esenciales en todo el mundo. Uno de los más tempranos tuvo lugar en Maroochy Shire, Queensland, Australia, en 2001: un *hacker* atacó una planta de tratamiento de aguas residuales. Se apoderó de los sistemas de control industriales de las instalaciones y «ocasionó que millones de litros de aguas negras sin tratar brotaran en parques

públicos, ríos e incluso en los terrenos de un hotel Hyatt Regency»[8]. El ataque destruyó cantidades importantes de flora y fauna marina local, por no hablar de la amenaza ambiental que supuso para los habitantes de la zona.

Tal vez uno de los sistemas más importantes vulnerables a ataques sea el tendido eléctrico de un país. Sin electricidad, las forjas del mundo moderno dejarían de funcionar: adiós a la luz, a los ascensores, a los cajeros automáticos, al control de tráfico, al metro, a las puertas electrónicas de los garajes, a las neveras y a las gasolineras. Y cuando las baterías de refuerzo y los generadores de emergencia acabaran agotándose, cosa que sucedería de manera inevitable en un momento u otro, adiós también a los teléfonos móviles y a Internet. Pese a nuestra dependencia absoluta de la electricidad en tanto que infraestructura tecnológica fundamental de nuestras vidas contemporáneas, el exsecretario de Defensa estadounidense Leon Panetta destacó que «el próximo Pearl Harbor que afrontemos podría ser perfectamente un ciberataque que paralice» los sistemas de energía y la red eléctrica[9].

Las preocupaciones de Panetta parecieron quedar validadas y apuntaladas por un informe del Departamento de Energía estadounidense, en el cual se señalaba que el tendido energético de Estados Unidos, al que a menudo nos referimos como «la máquina más compleja del mundo», conecta cinco mil ochocientas centrales eléctricas individuales y cuenta con más de 735 000 kilómetros de líneas de transmisión de alto voltaje. Y pese a ello, el 70 por ciento de los componentes clave de la red tienen más de veinticinco años de antigüedad[10]. Cada uno de estos componentes emplea tecnologías SCADA antiguas fáciles de sabotear contra las cuales se perpetran ataques continuos.

Una investigación acometida por el House Energy and Commerce Committee reveló que «más de una docena de empresas de servicios públicos informaban de ciberataques “diarios”, “constantes” o “frecuentes” que englobaban desde *phishing* hasta infecciones con *software* malicioso y sondeos hostiles. Una empresa de servicios públicos aseguró haber sido objeto de más de 10 000 intentos de ciberataques cada mes»[11]. El informe concluía que tanto gobiernos extranjeros como delincuentes y *hackers* aleatorios se esforzaban por planificar ataques o intentar sabotear la red. Estos hallazgos se añadían a declaraciones previas realizadas por agentes de los servicios de inteligencia al *Wall Street Journal*, en las que confirmaban que los ciberespías «habían penetrado el tendido eléctrico de Estados Unidos y habían dejado a su paso programas que podían afectar el sistema»[12]. Aquellos mismos agentes incluso afirmaban que espías rusos y chinos supuestamente habían cartografiado el tendido eléctrico estadounidense para «poder desactivar» la red en caso de sobrevenir tiempos de crisis o guerra.

Los terroristas también cuentan con estrategias para atacar digitalmente las infraestructuras de Estados Unidos. En el verano de 2012, el FBI desveló un vídeo emitido por el ala de medios de comunicación de Al Qaeda, As Sahab. En el vídeo, la

organización terrorista llamaba a sus «“muyaidines encubiertos” a llevar a cabo oleadas de ciberataques contra las redes estadounidenses tanto de estructuras gubernamentales como esenciales para la vida, incluido el tendido eléctrico»[13]. Anteriormente, investigaciones del FBI habían revelado numerosos intentos de Al Qaeda de realizar investigaciones y operaciones de vigilancia online en los sistemas de teléfonos de emergencias, centrales eléctricas, instalaciones de distribución de agua, centrales nucleares y depósitos de gas de Estados Unidos[14].

La organización terrorista incluso había completado elaborados informes acerca de las potenciales infraestructuras básicas a atacar, los cuales contenían desde fotografías de los objetivos hasta notas detalladas e investigaciones en línea.

Los *hackers* también se esfuerzan por entender, exponer y explotar las vulnerabilidades de SCADA y otras infraestructuras de información esenciales. Durante el Congreso de Comunicación Caos, un certamen de piratas informáticos celebrado en Alemania, los analistas de Positive Research demostraron cómo hacerse con el control pleno de infraestructuras industriales en los sectores del gas, la industria química, el petróleo y la energía[15]. Igual de inquietante es el hecho de que los piratas informáticos compartan esta información entre sí e incluso hayan creado bases de datos públicas de los fallos conocidos, bases de datos que puede consultar cualquiera y utilizar para controlar infraestructuras básicas. Una conocida base de datos de esta índole, Shodan, proporciona consejos sobre cómo aprovechar las vulnerabilidades para manejar cualquier cosa, desde centrales eléctricas hasta turbinas eólicas, permite efectuar búsquedas por país, empresa o dispositivo, y provee información de uso detallada y desciende enormemente el baremo técnico y de conocimientos necesario para que cualquier canalla sabotee infraestructuras básicas para las vidas de la población[16]. Así, para los atacantes interesados en hacerse con el control de nuestro mundo conectado, Shodan se ha convertido en su Google, un motor de búsqueda prácticamente imposible de clausurar porque está albergado en múltiples servidores en distintos países y la publicación de vulnerabilidades actualmente no se considera delito en la mayoría de ellos.

Las mafias también están concentrando su atención en los ataques a las infraestructuras como un medio lógico de extorsionar fondos a las empresas de servicios públicos y gobiernos. Entre 2005 y 2007 se produjeron varios incidentes de este tipo en Brasil, cuando tuvo lugar una oleada de ciberataques en el norte de Río de Janeiro y en el estado de Espírito Santo[17]. En aquel incidente, cerca de tres millones de personas quedaron sumidas en la oscuridad cuando la empresa de suministro eléctrico de la zona rehusó aceptar las exigencias de extorsión de un sindicato de la mafia local. Como resultado, la ciudad de Vitória, una de las mayores productoras de mineral de hierro del mundo, se vio obligada a desconectar numerosas fábricas, cosa que costó a la empresa cerca de siete millones de dólares. Los ataques fueron confirmados por agentes de la inteligencia estadounidense, investigadores en materia de seguridad y, de manera tangencial, por el propio presidente Obama,

cuando dijo: «Sabemos que… en otros países… ciberintrusos han sumido en la oscuridad a ciudades enteras»[18].

WHOIS: ¿quién está ahí?

El famoso general chino Sun Tzu, autor de *El arte de la guerra*, observó inteligentemente 2500 años antes de la creación de Internet que «si conoces a tu enemigo y te conoces a ti mismo, no correrás peligros ni aunque libres cien batallas». De acuerdo con esta afirmación y con vistas a entender las inmensas amenazas tecnológicas que afrontamos, es imperativo que entendamos a nuestros enemigos. Cada uno de ellos tiene distintos medios y motivos, pero también tienen algo en común: el riesgo que suponen para el mundo profundamente interconectado en el que vivimos.

El elenco de personajes responsables de ciberactividades ilícitas es muy amplio e incluye desde Estados nación hasta matones de barrio, grupos mafiosos transnacionales, servicios de inteligencia extranjeros, *hacktivistas*, personal militar, cibercombatientes, paramilitares patrocinados por los gobiernos, *script kiddies*[*], *hackers* de diversa índole, *phreakers*[*], piratas informáticos diversos, expertos decepcionados y espías industriales. Cada uno de ellos desempeña su papel en lo que el ejército estadounidense ha declarado el «quinto ámbito» de la batalla: el ciberespacio (tras la militarización de tierra, mar, aire y el espacio por parte de la generación pasada[19]).

Todos ellos suelen utilizar tácticas similares, aunque con distintos grados de sofisticación. No obstante, todos los atacantes se benefician de la naturaleza asimétrica de la tecnología: el defensor debe construir una muralla perfecta para bloquear el paso a todos los intrusos, mientras que el atacante sólo precisa encontrar una rendija en la armadura por la que colarse para perpetrar su asalto. Entre las facciones que combaten en el ciberespacio se da cooperación, voluntaria e involuntaria, pues los jugadores suelen aprender e imitar los éxitos operativos recíprocos. Por ejemplo, las mafias transnacionales utilizan operaciones de reconocimiento altamente sofisticadas para planificar sus ataques, si bien acostumbran a recurrir a matones de barrio para desempeñar algunas partes de sus tramas, como la colocación de colectores o desencriptadores de tarjetas de crédito en los cajeros automáticos, el blanqueo de dinero o el tráfico de los objetos robados en eBay. Las organizaciones terroristas aprenden de los ciberdelincuentes y realizan sabotajes para obtener fondos económicos y financiar sus operaciones en el mundo real. Países como China, Rusia e Irán forman cibercuadrillas de ciudadanos patriotas a sueldo del Estado, los cuales cuentan con la aprobación tácita, financiación y

formación a cargo del Gobierno. Y al hacerlo comparten algunas de las técnicas y herramientas que usan sus jefes gubernamentales. En el ciberespacio se da una simbiosis soterrada y existen metodologías comunes a todo el espectro de agentes amenazantes.

Quizá la primera imagen que nos viene a la mente a la hora de pensar en un pirata informático sea la estereotípica de un adolescente encerrado en el sótano de casa de su madre que aporrea el teclado sin descanso rodeado de bolsas de Fritos y latas de la Coca-Cola vacías e intenta cambiar sus notas infiltrándose en los ordenadores del instituto (como hacía Matthew Broderick en la película de 1983 *Juegos de guerra*). En los albores de la piratería informática, los sistemas telefónicos representaban la diana de los denominados *phreaks*, quienes manipulaban las redes para evitar los costes desorbitados de las llamadas a larga distancia. Recordemos a dos piratas informáticos que pasaron parte de su juventud en 1971 construyendo Blue Boxes o «cajas azules», o sea, dispositivos capaces de sabotear la red telefónica y efectuar llamadas gratuitas: Steve Wozniak y Steve Jobs[20]. Aquel dúo vendía cajas azules a los estudiantes de la Universidad de California en Berkeley como medio de conseguir el dinero con el que acabarían montando su pequeña empresa, la empresa de ordenadores Apple.

Con el paso del tiempo fueron surgiendo algunos otros *hackers* destacables, entre ellos Kevin Mitnick y Kevin Poulsen[21]. Mitnick es célebre por haberse infiltrado en los ordenadores de la empresa Digital Equipment Corporation a los dieciséis años de edad y realizar una serie de ciberintrusiones del mismo estilo que suscitaron la ira del FBI y le merecieron la distinción de ser el «*hacker* más buscado de Estados Unidos». La ingeniosa infiltración de Poulsen en 1990 le permitió hacerse con el control de todas las líneas telefónicas de una emisora de radio de Los Ángeles para asegurarse de ser el oyente número 102 en llamar y obtener así el premio máximo, un Porsche 944 S2 valorado en 50 000 dólares[22].

Estos ataques de las décadas de 1970, 1980 y 1990 se antojan casi benignos en comparación con los estándares actuales. En los años intermedios, los piratas informáticos se han organizado y han formado sindicatos mafiosos globales en línea. Cometen desde suplantación de identidades hasta fraudes con tarjetas de crédito, fraudes a la sanidad, fraudes al Estado del bienestar y fraudes fiscales. El crimen organizado persigue objetivos cada vez más importantes y sofisticados, incluidas las vastas cantidades de propiedad intelectual creadas por empresas de todo el mundo, desde los planes de productos de una compañía hasta el código fuente de sus ordenadores. A título de ejemplo, en octubre de 2013, unos piratas informáticos atacaron Adobe Systems en el Silicon Valley y robaron treinta y ocho millones de nombres de usuarios y contraseñas de cuentas, además de millones de números de tarjetas de crédito[23]. Hasta aquí, nada nuevo. La novedad de aquel ataque consistió en que los delincuentes también robaron más de cuarenta gigabytes del código fuente de los programas informáticos abanderados de Adobe, incluidos entre ellos:

Photoshop, ColdFusion y Acrobat[24].

Como resultado, los delincuentes no sólo estaban en disposición de vender libremente productos de Adobe, sino que podían alterar el código e insertar números incalculables de puertas traseras ocultas, *malware* y *exploits* o vulnerabilidades adicionales al producto, provocando con ello que los clientes legítimos y desprevenidos de Adobe pudieran sufrir una amplia variedad de ataques informáticos y robos de identidad, una evolución preocupante, dada la gigantesca huella digital global que Adobe tiene entre los usuarios informáticos. Incluso a Symantec, creadora de pcAnywhere y Norton AntiVirus, le han robado el código fuente. En efecto, la empresa que le vende a usted programas antivirus para protegerlo de ataques quedó en jaque cuando un pirata informático robó 1,27 gigabytes del código fuente de su *software* de seguridad y exigió la cifra relativamente irrisoria de 50 000 dólares a cambio de no publicar los datos en el conocido sitio web de *hackers* The Pirate Bay[25].

Las delincuencia organizada tradicional, como la mafia italiana, la yakuza japonesa, las tríadas chinas o los cárteles del narcotráfico colombianos han desviado esfuerzos y recursos de sus actividades delictivas habituales para sacar partido a los beneficios fáciles, el anonimato y el escrutinio policial limitado que ofrece el ciberespacio[26]. Además, no tienen que preocuparse por las draconianas sentencias mínimas a menudo relacionadas con sus antiguas actividades económicas, como el tráfico de personas o el contrabando de narcóticos. Las mafias del ciberespacio son responsables del envío de correo no deseado, *phishing*[*], anuncios falsos de productos farmacéuticos, diseminación de imágenes de pedofilia y pederastia, ataques por denegación de servicio y extorsión, por mencionar algunas de sus actividades predilectas.

Además de la vieja guardia incondicional de la delincuencia organizada, está apareciendo en escena un nuevo tipo de organizaciones de ciberdelincuencia con un juego más astuto[27]. Estos grupos criminales emergentes de piratas informáticos profesionalmente organizados generan pingües beneficios y son auténticamente mundiales, con grandes concentraciones en China, Indonesia, Estados Unidos, Taiwán, Rusia, Rumanía, Bulgaria, Brasil, India y Ucrania. Nuevos sindicatos, como la Russian Business Network (RBN) en San Petersburgo, incluso se han hecho un nombre como organizaciones de ciberdelincuencia con líneas multiproducto y servicios integrales[28].

La RBN es célebre, entre otras cosas, por proporcionar servicios de hospedaje de sitios web «blindados» a toda suerte de empresas delictivas y no se inmiscuye en absoluto en el contenido que alberga, que puede ser desde pornografía infantil hasta intercambio de vulnerabilidades de *software* malicioso a través de sus servidores[29]. Otros grupos delictivos profesionales de *hackeo*, como ShadowCrew, ofrecen paraísos virtuales para *carders* («tarjeteros») especializados en el nebuloso mundo del

hurto de datos personales de identificación, incluidas contraseñas y permisos de conducir falsificados o tarjetas de crédito robadas, ingredientes clave para la creciente economía de la suplantación de identidad mundial. ShadowCrew operaba en el hoy desaparecido sitio web CarderPlanet.com, donde más de dos mil delincuentes de todo el mundo podían reunirse libremente para comprar y vender identidades, documentos y números de cuenta sustraídos y pirateados[30]. Fundado por el célebre pirata informático y delincuente Albert González, ShadowCrew ofrecía a otros delincuentes lecciones acerca de prácticamente cualquier materia, desde criptografía hasta técnicas de clonación de tarjetas, y se cree que la organización de González fue responsable del robo y la reventa de más de ciento ochenta millones de tarjetas de crédito y débito[31]. La cantidad y el alcance de estos anillos de la ciberdelincuencia organizada transnacional y sumamente provechosa han aumentado, y la empresa de seguridad CrowdStrike sigue el rastro activamente a más de cincuenta de estas grandes organizaciones en todo el mundo[32].

Además de los sindicatos de la delincuencia organizada transaccional, los *hacktivistas* (ciberatacantes con motivos políticos) constituyen uno de los grupos más influyentes y potentes del ciberespacio. Anonymous, LulzSec, AntiSec, WikiLeaks y el Ejército Electrónico Sirio se engloban dentro de esta categoría y lanzan ataques para vengar supuestas injusticias. Personajes famosos como Julian Assange, Chelsea (Bradley) Manning y Edward Snowden se han convertido en nombres populares por desafiar a algunas de las instituciones más poderosas del mundo y publicar datos que otros habrían preferido que permanecieran ocultos. Sin embargo, mientras que Assange, Manning y Snowden han ocupado las portadas de la prensa mundial, otros grupos *hacktivistas* prefieren que sus integrantes individuales permanezcan discretamente ocultos, subordinados a la organización en sí y a su amplio programa de actividades. Uno de los ejemplos más destacables es Anonymous, que se autodefine como una organización sin líderes cuyos miembros se dejan ver en público con máscaras de Guido Fawkes[33].

El lema del grupo: «Somos anónimos. Somos legión. No perdonamos. No olvidamos. Tendréis noticias nuestras» expresa sus valores: «Los corruptos nos temen. Los honestos nos respaldan. Los heroicos se unen a nosotros»[34]. Cuando MasterCard, Visa y PayPal llegaron al acuerdo de dejar de canalizar donaciones a la organización WikiLeaks de Julian Assange, Anonymous respondió lanzando una serie de ciberataques efectivos contra estas empresas financieras[35]. Anonymous se opone con vehemencia a lo que la organización percibe como leyes antipiratería rígidas y se acreditó un ataque anterior contra la red Sony PlayStation Network en respuesta al apoyo de Sony a la ley antipiratería de Estados Unidos conocida con el nombre de «*Stop* Online Piracy Act»[36].

Anonymous se concibe como una organización que realiza ataques informáticos para bien y ha asumido un amplio abanico de causas sociales, incluido el apoyo a

activistas en todo Oriente Próximo durante la Primavera Árabe[37]. Incluso algunos de los críticos más ardientes del grupo podrían sorprenderse defendiendo algunas de las actividades menos conocidas de Anonymous en la lucha contra las organizaciones criminales y la injusticia[38]. Por ejemplo, durante un ataque bautizado como «Operación Darknet», integrantes de Anonymous atacaron sitios web de pornografía infantil que contenían imágenes atroces de abusos sexuales a niños. El colectivo de piratas informáticos dejó sin conexión aquellos sitios web e hizo públicos los nombres de mil quinientos pedófilos que utilizaban sus servicios. Tanto si uno apoya como si deplora las acciones acometidas por Anonymous y otras organizaciones *hacktivistas*, hay algo claro: son una fuerza a tener en cuenta entre el amplio tapiz de agentes amenazantes en este mundo hiperconectado.

Los *hacktivistas* son capaces de atacar a cualquier persona o corporación y pueden tener un gran impacto geopolítico en el mundo, tal como se demostró durante la Primavera Árabe. En reconocimiento a su poder creciente, la revista *Time* incluyó a Anonymous entre las cien personas más influyentes del mundo en 2012[39]. Su influencia y sus capacidades en expansión no han pasado desapercibidas a los gobiernos, y recientemente se reveló que los Government Communications Headquarters (Cuartel General de Comunicaciones del Gobierno del Reino Unido, más conocido por sus siglas en inglés: GCHQ), el equivalente británico a la Agencia de Seguridad Nacional de Estados Unidos, había lanzado su propia serie de ataques de denegación de servicio contra Anonymous y sus miembros en un intento por interrumpir sus actividades[40]. Esta espectacular respuesta por parte de un Estado contra un agente no estatal y grupo activista demuestra la repercusión que Anonymous está teniendo en el mundo.

Entre tanto, las organizaciones terroristas también emplean de manera creciente Internet y otras tecnologías para planificar, respaldar y ejecutar sus actividades criminales[41]. La tecnología ayuda a los terroristas a reclutar nuevos miembros en foros encubiertos, a efectuar operaciones de financiación (mediante ciberdelincuencia y recaudación de fondos online), a comunicarse de manera clandestina y a distribuir propaganda, como los espantosos vídeos de decapitación que produce ISIS (el Estado Islámico). En ISIS son expertos en tecnología y en sus últimos vídeos de reclutamiento incluso incorporaron escenas del videojuego *Grand Theft Auto V* para mayor efecto. En su producción de vídeos online, este vil grupo terrorista ofrecía a los nuevos reclutas la oportunidad de «hacer lo que se hace en los juegos, pero en la vida real, en el campo de batalla […] como atacar un convoy militar o matar a agentes de policía»[42]. El vídeo lleva estampado el logotipo de ISIS.

La exploración y búsqueda en Internet por parte de terroristas es moneda corriente y en más de una ocasión se han encontrado imágenes de Google Earth de supuestos objetivos, incluido un plan de 2007 de hacer estallar los depósitos de combustible del Aeropuerto Internacional John F. Kennedy de Nueva York[43]. Los

terroristas han sido de los primeros en adoptar las tecnologías, sobre todo por lo que a encriptación de datos para garantizar sus comunicaciones se refiere. Por ejemplo, «Ramzi Yousef, el cerebro condenado por el primer bombardeo del World Trade Center en 1993, utilizó archivos encriptados para ocultar detalles de su plan de destruir once aviones de pasajeros estadounidenses»[44]. En el caso de Yousef, los cuerpos de seguridad tardaron más de un año en descifrar el algoritmo de encriptación empleado por el terrorista y, al hacerlo, afortunadamente la policía logró impedir los ataques contra los aviones.

Algunos expertos en contraterrorismo se han referido a Internet como una «universidad de terroristas», un lugar donde los terroristas pueden aprender nuevas técnicas y habilidades para perfeccionar sus metodologías de ataque. Hay disponibles en línea para cualquiera documentos como *The Mujahideen Poisons Handbook* («Manual de venenos para muyahidines»), que contiene diversas «recetas» para elaborar venenos caseros y gases venenosos[45]. Y la *Enciclopedia de la Yihad*, de seiscientas páginas de grosor, también puede consultarse ampliamente e incluye capítulos con títulos tan ilustrativos como «Cómo matar», «Dispositivos explosivos», «Cómo fabricar detonadores» y «Asesinato con minas». En un ejemplo espantoso de lo peligrosa que puede llegar a ser la educación virtual, Dzhokhar Tsarnaev, el terrorista sospechoso arrestado en relación con los bombardeos de abril de 2013 en la Maratón de Boston, admitió ante las autoridades que él y su hermano habían aprendido a fabricar la bomba con una olla a presión utilizada en su atentado tras leer las instrucciones paso a paso publicadas en la revista online de Al Qaeda *Inspire*, concretamente en un artículo titulado «Fabrica una bomba en la cocina de tu madre»[46].

Los terroristas no sólo utilizan Internet con fines de planificación y respaldo operativo, sino que también cometen acciones de piratería y ciberdelitos para financiarse y poder llevar a cabo sus actos terroristas en el mundo real. En junio de 2007, la policía del Reino Unido desactivó una célula de ciberterroristas y detuvo a tres habitantes británicos, Tariq al-Daour, Waseem Mughal y Younes Tsouli, acusados de usar Internet para incitar a matar. Las pruebas presentadas demostraban que los tres hombres habían utilizado cuentas de tarjetas de crédito sustraídas para adquirir artículos para otros yihadistas, como gafas de visión nocturna, dispositivos de posicionamiento global o GPS y tarjetas de prepago para teléfonos móviles, con la finalidad de proporcionar un apoyo táctico directo en operaciones terroristas. «Supuestamente, el trío realizó cargos fraudulentos por un total de más de 3,5 millones de dólares estadounidenses y contaba con una base de datos integrada por cerca de 40 000 cuentas de tarjetas de crédito robadas[47]».

Incluso el tristemente célebre cerebro de los bombardeos de 2002 en Bali, Imam Samudra, perteneciente al grupo terrorista vinculado con Al Qaeda Jemaah Islamiya, financió su ataque, en el que fallecieron más de 200 personas, con 150 000 dólares obtenidos mediante el pirateo de cuentas bancarias y líneas de crédito

occidentales[48]. Samudra era un experto en tecnologías y, mientras estaba en prisión, escribió un manifiesto autobiográfico que contenía un capítulo titulado: «Hackeo, ¿por qué no?»[49]. En el libro, Samudra compartía sus técnicas para piratear y «utilizar tarjetas de crédito fraudulentas» con sus discípulos, a quienes alentaba a «llevar la guerra santa al ciberespacio atacando ordenadores estadounidenses, con el objetivo concreto de cometer fraudes con tarjetas de crédito» con los cuales financiar sus operaciones. Los terroristas parecen haber captado el mensaje y tanto los atentados del 11-M de 2004 en la estación de trenes de Atocha, Madrid, donde 190 personas fallecieron y cerca de 2000 resultaron heridas, como los bombardeos del 7-J en Londres, en los que 52 civiles fueron masacrados y más de 700 resultaron heridos, se financiaron en parte o en todo mediante actividades fraudulentas con tarjetas de crédito[50].

A medida que las habilidades técnicas para el pirateo informático de las organizaciones terroristas progresan, también lo hace la cantidad de ganancias adquiridas ilícitamente que son capaces de generar online. Por ejemplo, a finales de 2011, la policía de Filipinas en colaboración con el FBI destapó una estafa de pirateo telefónico contra AT&T que defraudó a la empresa y a sus clientes empresariales unos dos millones de euros. La célula de piratas informáticos filipina colaboraba con Jemaah Islamiya y canalizó los millones para financiar al grupo terrorista con base en Arabia Saudí que, a su vez, financió a Lashkar-e-Toiba, el grupo terrorista con base en Pakistán responsable del letal asedio con bombardeo que en 2008 sacudió la ciudad de Bombay, India, y causó centenares de muertos y mutilados[51].

Es evidente que los delincuentes, *hacktivistas* y terroristas utilizan la interconectividad en nuestra contra, sea para obtener beneficios económicos, con fines políticos, sea, sencillamente, para perpetrar masacres. Son autodidactas en materia de ciencia y tecnología y han demostrado ser una fuerza formidable a la hora de aprovechar la naturaleza esencialmente insegura de nuestra piel tecnológica del siglo XXI. Ahora bien, los ladrones, *hackers*, activistas y terroristas no son los únicos habitantes de la clandestinidad digital. Los acompaña toda una falange de Estados nación, cibercombatientes y servicios de inteligencia de distintos países, cada uno de los cuales opera con astucia en el llamado quinto ámbito, inclinando en beneficio propio la inseguridad de la infraestructura digital subyacente que unifica el planeta.

Y aunque el internauta medio de hoy en día puede limitarse a actualizar su estado en Facebook o a jugar a los *Angry Birds*, conviene recordar que Internet la creó la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA en sus siglas en inglés), una invención del Departamento de Defensa estadounidense creada para garantizar la redundancia de las comunicaciones militares en caso de producirse un ataque nuclear[52]. Internet es una creación militar con el resultado de ramificaciones geopolíticas importantes.

Precisamente cuando los gobiernos destinan su atención (y sus presupuestos) a ciberoperaciones ofensivas podemos apreciar la gama íntegra de vulnerabilidades del

hardware y el *software* del cual dependemos y se expone por completo nuestra fragilidad tecnológica. Aunque una demanda de extorsión de 50 000 dólares a Symantec o incluso una pérdida a manos de la piratería de mil millones de dólares en Target sigan siendo notorios y nos llamen la atención, son *peccata minuta* en comparación con la brecha abierta en los sistemas informáticos del Pentágono que permitió espiar el proyecto del caza F-35 Joint Strike Fighter, valorado en trescientos millones de dólares, el programa de armamento más caro de la historia del Departamento de Defensa de Estados Unidos[53].

En mayo de 2013, la Administración estadounidense señaló específicamente a China como responsable de una serie de ataques contra sistemas vitales para el gobierno y la defensa de Estados Unidos, incluido el F-35[54]. A lo largo de los años se ha informado del robo de otros anteproyectos y tecnologías de defensa, incluidas las de un sistema avanzado de misiles Patriot conocido como PAC-3, el sistema Aegis Ballistic Missile Defense de la Marina estadounidense, el caza-bombardero F/A-18, el V-22 Osprey, el helicóptero Black Hawk y el buque de combate litoral[55]. De acuerdo con un informe del FBI, China ha constituido en secreto un ejército de 180 000 ciberespías y combatientes que han realizado la asombrosa cifra de noventa mil ataques informáticos sólo contra la red del Departamento de Defensa de Estados Unidos[56]. La totalidad de estos robos y su repercusión en la seguridad nacional del país es sobrecogedora.

Las supuestas actividades de ciberpirateo que practica China le proporcionan ventajas estratégicas importantes, como una ventaja operativa y táctica inmediata en cualquier conflicto con Estados Unidos. Contar con los anteproyectos de tantos sistemas de defensa estadounidenses aporta datos clave acerca de cómo funcionan y, lo más relevante, de cómo derrotarlos en tiempos de crisis. Además, este gigantesco «robo de cerebros» ahorra a China miles de millones de dólares en investigación de sus propios costes de desarrollo militar (y décadas de trabajo) por el mero hecho de apropiarse y evolucionar a partir de un trabajo pagado por los contribuyentes estadounidenses.

Por supuesto, China no sólo apunta a la tecnología militar de Estados Unidos, sino a una letanía de instituciones de Washington, incluidas entre ellas despachos de abogados, grupos de expertos, grupos defensores de los derechos humanos, contratistas, oficinas de congresistas, embajadas y diversos organismos federales[57]. Más aún, un informe realizado en 2009 por investigadores canadienses del Infowar Monitor, el SecDev Group y el Citizen Lab de la Universidad de Toronto desveló la existencia de la llamada GhostNet, «una inmensa red de ciberespionaje mundial» que se extendía a 103 países, se controlaba mediante servidores en China y tenía por objetivos al gobierno tibetano en el exilio y al propio Dalai Lama[58].

China ha sido acusada también de piratear numerosos medios de comunicación, incluido el famoso episodio del *New York Times* a principios de 2013, después de que el diario informara de que unos parientes del primer ministro chino, Wen Jiabao,

habían acumulado una riqueza de miles de millones de dólares mediante sus acuerdos empresariales desde que Wen ocupaba el cargo[59]. Aquella infiltración ofreció a los atacantes acceso a todos los ordenadores del *New York Times* y se especula con que los chinos intentaban descubrir las fuentes y los contactos que podían dañar las reputaciones de sus líderes. El diario *Times* contrató a la empresa privada de ciberseguridad Mandiant, que investigó el incidente y, en un fascinante informe, vinculaba el ataque con la Unidad 61 398 del Ejército de Liberación Popular[60]. Los cuarteles generales de la unidad, situados en la calle Datong, en el distrito de Pudong en Shanghái, ocupan un edificio de doce plantas y doce mil metros cuadrados al cual miles de empleados acuden a diario con el objetivo de infiltrarse ilegalmente y espiar a gobiernos, empresas y personas de todo el mundo.

Estos hurtos tecnológicos, que el Estado chino no comete en persona, suelen estar patrocinados por el gobierno, los ejecutan intermediarios designados, tienen hondas repercusiones y representan graves costes para empresas de todo el mundo. En 2012, *Bloomberg Businessweek* publicó en portada un reportaje acerca del robo de propiedad intelectual mundial continuo que realiza China con un titular de gran tamaño que rezaba: «¡Eh, China! Deja de robarnos»[61]. El reportaje incluía la historia de Dan McGahn, el director ejecutivo de American Superconductor (AMSC), con sede en Massachusetts, una empresa de tecnologías energéticas ecológicas especializada en el diseño de sistemas eléctricos y del *software* que hace funcionar turbinas eólicas de gran tamaño. En marzo de 2011, el principal cliente de AMSC, el Sinovel Wind Group, antiguamente propiedad estatal china, empezó a rechazar sin previo aviso las entregas en su planta de ensamblaje en la provincia de Liaoning y canceló más de 700 millones de dólares en pedidos pendientes de envío realizados a AMSC. La respuesta del mercado a los pedidos cancelados a AMSC fue brutal: un descenso del 40 por ciento en su valoración en un solo día y un declive del 84 por ciento en septiembre de aquel año.

La investigación del asunto reveló que las turbinas de Sinovel «parecían funcionar con una versión robada del *software* de AMSC» y que la empresa china había hurtado una copia completa del código fuente informático propiedad de la empresa estadounidense. Puesto que Sinovel poseía todos los conocimientos de AMSC, podía prescindir de AMSC y sus productos y producirlos por sí misma. De ahí que la empresa china cancelara los contratos de provisiones existentes por valor de más de 700 millones de dólares a la empresa de Massachusetts.

En total, entre los robos de propiedad intelectual comercial, gubernamental y militar, las actividades de pirateo de China han proporcionado al país la mayor transferencia de riqueza de toda la historia de la humanidad[62]. De acuerdo con el informe de Akamai *State of the Internet*, un alarmante 41 por ciento de todos los ciberataques que se producen en el mundo tienen su origen en China[63]. Por descontado, China niega de manera vehemente y rutinaria su implicación en cualquier actividad de pirateo mundial. Y cuando aparecen alegaciones, el portavoz

de la embajada china en la capital del país pirateado en cuestión, ya sea París, Berlín o Nueva Delhi, repite una misma consigna. El mensaje emitido por un oficial de la embajada china en Washington, D. C., llamado Wang Baodong es una respuesta prototípica: «China se opone firmemente a las actividades de pirateo internacional y está dispuesta a colaborar con otros países para garantizar la seguridad del ciberespacio»[64]. No es la primera vez que se esgrime una respuesta como la de Wang. Si se busca en Google la frase «China denies *hacking*» («China niega el pirateo») se obtienen unos treinta y cinco millones de ejemplos de tal negación. Agua de borrajas.

Ahora bien, aunque China es el país más poblado de la Tierra, no es el único que lleva a cabo ciberoperaciones. De acuerdo con el exdirector del FBI Robert Mueller, había al menos 108 países, entre ellos Irán, dotados de unidades dedicadas a los ciberataques cuyo fin era recabar secretos industriales e infiltrarse en infraestructuras esenciales[65]. A finales de 2012, un grupo de piratas informáticos desconocido llamado Cutting Sword of Justice se responsabilizó de llevar a término el sabotaje informático más destructivo contra una empresa perpetrado hasta entonces al atacar al gigante saudí del petróleo y el gas Aramco[66]. La ofensiva tuvo lugar en la víspera de una de las noches más sagradas del calendario islámico, la Noche del Destino, cuando se cree que Mahoma reveló el Corán a sus discípulos. Con ocasión de aquella festividad, los cincuenta y cinco mil empleados de la empresa se hallaban en sus hogares festejando con sus familiares y amistades. En juego: 260 mil millones de galones de petróleo, valorados en más de 8000 billones de dólares (catorce veces la capitalización bursátil de Apple Inc.).[67]

Durante el incidente, un infiltrado desconocido con acceso a las instalaciones insertó una unidad de USB infectada en un único PC conectado a la red informática de la empresa. En cuestión de minutos, la carga explosiva del virus de la unidad, conocido como Shamoon, se extendía como un incendio forestal por los treinta mil ordenadores corporativos de Aramco[68]. Pese a que su objetivo era interrumpir la producción de petróleo y gas de las instalaciones de Aramco, las buenas prácticas en materia de seguridad conllevaron que el virus «sólo» destruyera datos corporativos. ¿El peaje? Shamoon borró el 75 por ciento de los treinta mil discos duros de la empresa, eliminando con ello «documentos, hojas de cálculo, correo electrónico, archivos… y sustituyéndolo todo con una imagen de una bandera estadounidense en llamas»[69].

El grupo Cutting Sword of Justice afirmó que su ataque era una respuesta a los «crímenes y atrocidades» cometidos por los saudíes en Siria y en Bahréin contra los manifestantes chiíes[70]. Los agentes de la inteligencia estadounidense sospechan que Cutting Sword of Justice no es más que una tapadera de Irán, a quien consideran culpable de patrocinar el ataque[71]. Las asombrosas capacidades informáticas demostradas en el ataque a Aramco precedieron a otros ataques con éxito realizados

por el gobierno iraní, incluida una serie de interrupciones por ataques distribuidos de denegación de servicios (DDoS) a comienzos de 2013 contra el sector de los servicios financieros de Estados Unidos. Numerosas entidades bancarias —incluidas JPMorgan Chase, Bank of America, Wells Fargo, BB&T, HSBC y Citigroup— se vieron afectadas por el ataque, que dejó a sus redes corporativas y sus sitios web públicos inaccesibles durante largos períodos e impidió a los clientes acceder a su dinero[72]. Un grupo de piratas informáticos autodenominado Izz ad-Din al-Qassam Cyber Fighters se responsabilizó del ciberbombardeo, pero las autoridades estadounidenses opinan que el grupo no es más que un intermediario que actúa en nombre de Irán[73].

El ataque de denegación de servicio generalizado perpetrado contra el sector financiero estadounidense por Irán fue alarmante por sus dimensiones y su alcance, y por el colosal volumen de datos generado por quienes lo realizaron[74]. «Algunos bancos padecieron un flujo de tráfico sostenible que ascendía a 70 gigabits» por segundo. Para situar ese volumen de tráfico DDoS en perspectiva, es como si mil millones de personas telefonearan simultáneamente a un banco, colgaran y volvieran a marcar un segundo después. Para que la llamada (o visita al sitio web) de alguien fuera conectada, debería ser el número 1 000 000 001 de la lista. En otras palabras: por muchos intentos que hiciera, jamás contactaría con el banco[75].

Lo más sorprendente, no obstante, es que se comunicó que el ataque respaldado por Irán contra el sector de servicios financieros superaba en varias veces al infame ataque de 2007 contra la nación de Estonia perpetrado por unos piratas informáticos afincados en Rusia, que prácticamente dejó sin conexión a todo el pequeño país báltico. Existe la creencia generalizada de que aquel incidente se llevó a cabo con el apoyo del gobierno ruso a través de *hackers* subcontratados después de que Estonia decidiera trasladar una lápida de la era soviética del lugar que había ocupado siempre en el centro de la ciudad de Tallin hasta las afueras de la población, movimiento que indignó a Moscú. Muchos expertos en seguridad clasificaron aquel ataque digital sin cuartel contra Estonia como la «primera ciberguerra del mundo», debido a su envergadura y espectro. Dado que Irán acababa de superar aquel ataque, un investigador en temas de seguridad comentó que los bombardeos técnicos de la República Islámica habían pasado de ser «poco más que unos chihuahuas dando ladridos a convertirse en una manada de Godzillas que soltaban fuego por la boca»[76].

Por supuesto, también se ha acusado multitud de veces a Estados Unidos de acometer acciones de piratería informática contra el resto del mundo, la mayoría de ellas basadas en los numerosos documentos clasificados y revelados de manera unilateral por el extrabajador independiente de la Agencia de Seguridad Nacional (NSA en sus siglas en inglés) Edward Snowden a partir de junio de 2013. Snowden informó con todo lujo de detalles del aparato de vigilancia técnica mundial operado por la Agencia de Seguridad Nacional y proporcionó pruebas documentales para respaldar sus afirmaciones en conversaciones con los periodistas Glenn Greenwald y

Laura Poitras. Posteriormente salieron a la luz programas como PRISM y XKeyscore, así como la supuesta capacidad de la NSA de rastrear miles de millones de mensajes de correo electrónico, mensajes de teléfono, sesiones de chat y SMS cada día[77].

Mientras vivía en Moscú, Rusia, donde le había sido concedido el asilo temporal, Snowden continuó catalogando las operaciones técnicas y cibernéticas ofensivas de Estados Unidos, incluidas las escuchas telefónicas de los móviles personales de líderes mundiales que englobaban desde la canciller alemana Angela Merkel hasta la presidenta brasileña Dilma Rousseff[78]. Más aún, Snowden divulgó que la NSA grababa las comunicaciones de millones de ciudadanos de todos los países, incluidos Francia y Alemania, con un total de 120 mil millones de llamadas al mes en todo el mundo[79]. Las filtraciones de Snowden también cercenaron la comprensión que la comunidad internacional había mostrado hacia las quejas de Estados Unidos con respecto a los ciberataques intensivos perpetrados en su contra por parte de la República Popular de China, sobre todo cuando reveló que los estadounidenses también habían lanzado ciberoperaciones contra objetivos chinos, incluidos China Mobile y la prestigiosa Universidad de Tsinghua[80]. Dependiendo de las convicciones políticas de cada cual y del punto de vista personal, Snowden puede considerarse un enemigo del Estado, un héroe, un chivato, un disidente, un traidor o un patriota. Ahora bien, al margen de cómo lo juzgue la historia, sus revelaciones, en caso de ser ciertas, pintan un retrato muy detallado de cómo los gobiernos se están apuntando a la ciberguerra.

Un análisis del panorama de los agentes amenazantes que pueblan el ciberespacio revela la existencia de *hacktivistas*, delincuentes, combatientes intermediarios, terroristas y gobiernos corruptos, todos ellos perfectamente capaces de aprovechar los fallos en la seguridad de las infraestructuras tecnológicas de nuestro mundo. Nuestros datos financieros, nuestra identidad, las fotografías de nuestros hijos y los tendidos eléctricos de los distintos países son vulnerables y se encuentran en riesgo, convertidos en objetivos fáciles de atacar. Con todo, por ubicua que parezca la tecnología en nuestras vidas actuales, su tasa exponencial de crecimiento implica que en el horizonte se perfila un tsunami de avances tecnológicos que nos dejará atónitos. No sólo el ancho y largo de nuestra conexión a la red de información global se expandirán enormemente, sino que nuevas tecnologías hasta ahora relegadas al ámbito de la ciencia ficción no tardarán en emerger como ciencia empírica. En resumen, no hemos visto nada todavía.

Capítulo 3

Moore: fuera de la ley

> El futuro ya está aquí. Lo que ocurre es que aún no está repartido de manera uniforme.
>
> WILLIAM GIBSON, *Neuromante*

Para entender el valor matemático de los exponentes y las curvas exponenciales, a los escolares de Francia se les solicitó que imaginaran un estanque en el que había brotado una pequeña hoja de un nenúfar. La hoja, se les dijo, duplicaría su tamaño cada día y tardaría treinta días en cubrir todo el estanque. Si el nenúfar cubría todo el estanque, asfixiaría y mataría al resto de formas de vida subacuáticas. La pregunta que se les formuló a los estudiantes fue: ¿qué día cubriría el nenúfar la mitad del estanque?

Al principio, no había de qué preocuparse. El nenúfar crecía a un ritmo apenas apreciable, y para el día 20 aún no había cubierto más que una décima parte del uno por ciento del estanque. Sólo el 0,1 por ciento. Cinco días más tarde, alcanzó el 3 por ciento, pero seguía sin ser objeto de preocupación, de manera que los niños dejaron que continuara creciendo. Hasta que, de repente, el día 29, el nenúfar cubrió la mitad del estanque. Para entonces, apenas había margen de maniobra para salvar el estanque, que quedó asfixiado al día siguiente por el nenúfar. El día 29 podía parecer como otro día cualquiera, pero, dada la naturaleza de los exponenciales, el estanque estaba a punto de quedarse sin aire y perecer.

Las lecciones que nos enseña este ejemplo del estanque son que la naturaleza mágica del crecimiento exponencial puede avanzar a hurtadillas muy, muy rápidamente y que nuestro pensamiento lineal puede ponernos en peligro.

El mundo exponencial

En su libro *The Singularity Is Near*, el futurista Ray Kurzweil describe la naturaleza exponencial del mundo tecnológico que nos rodea y nos presenta el concepto de lo que él denomina «la rodilla de una curva exponencial». La rodilla de la curva es un punto de inflexión en el tiempo en el que una tendencia exponencial deviene evidente. Al cabo de poco, esa línea de tendencia se vuelve explosiva y se muestra esencialmente vertical cuando se percibe el impacto matemático del crecimiento

exponencial. Malcolm Gladwell describe este fenómeno como un «punto de inclinación» en el que la suma de las pequeñas cosas conlleva una diferencia masiva y destacable en los resultados. Dada la naturaleza exponencial de la tecnología y su omnipresencia en nuestras vidas, abundan las pruebas de que nos aproximamos aceleradamente a un punto de inflexión de estas características. La pregunta es: ¿nos inclinaremos hacia el bien o hacia el mal?

De acuerdo con la Unión Internacional de Telecomunicaciones (ITU en sus siglas en inglés), en el año 2000 había sólo 360 millones de personas conectadas a Internet[1]. Pese a que tardó casi cuarenta años en desarrollarse, en 2005 esa comunidad global que es Internet alcanzó sus primeros mil millones de usuarios[2]. Dicha cifra se duplicó al cabo de sólo seis años, en marzo de 2011, todo un hito. El crecimiento más importante se ha registrado en el mundo en vías de desarrollo, donde Asia y África experimentan un ascenso del 841 por ciento y un vertiginoso 3606 por ciento respectivamente desde 2000[3]. Y, mientras que la mitad del mundo por desgracia aún no tiene acceso a Internet, el presidente ejecutivo de Google, Eric Schmidt, se ha aventurado a predecir que en 2020 todo el mundo estará en línea[4].

El ritmo implacable al cual tienen lugar estos cambios y la presencia en expansión perpetua de la tecnología en nuestras vidas se han catalizado mediante un axioma de la tecnología conocido como la ley de Moore. Esta ley debe su nombre a Gordon Moore, el expresidente de Intel Corporation, célebre porque ya en 1965 predijo que el número de transistores por metro cuadrado en un circuito integrado se duplicaría cada año en el futuro[5]. Este principio, que más tarde se corrigió de manera que tal duplicación se da entre cada dieciocho meses y dos años, se conoce como ley de Moore y, en general, se aplica ampliamente a la potencia y las capacidades de las tecnologías basadas en circuitos. Como resultado de ello, el espectro creciente de descubrimientos científicos, que abarcan desde la biotecnología hasta la robótica, se rige por la ley de Moore y sus consecuencias. La ley de Moore también tiene implicaciones allende la ciencia, en ámbitos que engloban desde la geopolítica hasta la economía, pues la tecnología cada vez afecta a más esferas de la existencia humana. Pero lo más importante es que la ley de Moore puede tener repercusiones tanto positivas como negativas en nuestro mundo.

Precisamente esa duplicación persistente de la capacidad de procesamiento de los ordenadores estipulada en la ley de Moore la hace tan trascendental. Significa que todas las tecnologías basadas en la informática presentan curvas de crecimiento exponenciales, en lugar de lineales. Dicho de otro modo: estas tecnologías no responden a sumas, sino a multiplicaciones. Es la diferencia entre 1, 2, 3, 4, 5, 6, 7 y 2, 4, 8, 16, 32, 64, 128. Cuanto más se alarga la tendencia lineal frente a la exponencial, más inexorables y alarmantes se vuelven los resultados. Para poner este concepto en perspectiva, si uno da treinta pasos linealmente, puede atravesar el salón. Pero, si diera treinta pasos exponencialmente, es decir, si duplicara la distancia con cada paso sucesivo, viajaría entre la Tierra y la Luna. El hecho de que las tecnologías

actuales presenten curvas de crecimiento exponenciales en lugar de lineales es fundamental para entender la siguiente fase de la evolución humana. Vivimos en tiempos exponenciales.

A medida que las tecnologías de la información continúan duplicando su rendimiento, capacidad y ancho de banda, cosas asombrosas devienen posibles. Pongamos por ejemplo el iPhone que cientos de millones de usuarios llevan en sus bolsillos a diario. Aunque parezca increíble, literalmente tiene más potencia de procesamiento informático de la que tenía toda NASA cuando el *Apollo 11* alunizó hace cuarenta años[6]. Los teléfonos inteligentes modernos, los *smartphones*, son más de «un millón de veces más baratos y miles de veces más rápidos que un superordenador de la década de 1970»[7]. Como resultado de las repercusiones matemáticas de los exponenciales y la ley de Moore, «en el siglo XXI, no experimentaremos cien años de progreso en el siglo, sino más bien veinte mil (al ritmo actual)»[8].

Dado el ritmo de cambio exponencial en la sofisticación y potencia de procesamiento de los ordenadores, debería ser obvio que en el futuro muy próximo los ordenadores presentarán unas capacidades asombrosas. Ray Kurzweil describe la duplicación constante en la potencia y el rendimiento del precio de la informática en su «ley de retornos acelerados»[9]. Vaticina que en un punto del tiempo se producirá una singularidad tecnológica o, dicho de otro modo: que en un momento puntual el progreso informático será tan veloz que superará la capacidad de la humanidad para asimilarlo y la inteligencia de las máquinas excederá a la inteligencia humana. Tanto si ese día llega como si no (la predicción de Kurzweil es que se producirá en el año 2045), hay algo claro: la capacidad de procesamiento crece de manera exponencial a la par que nuestra habilidad para entender la red de información global y cartografiar sus inmensas interconexiones mengua.

No es cuestión de imaginación: la tecnología progresa a mucha más velocidad de lo que la mayoría somos capaces de asimilar, y no hay que sentirse culpable por ello. Hasta la fecha, los seres humanos hemos evolucionado para pensar de manera lineal; el pensamiento lineal está codificado en nuestro cerebro desde el amanecer de la humanidad. Desde nuestros días en las llanuras del Serengueti, hemos realizado de manera intuitiva cálculos lineales mentales para determinar la mejor vía de escape de un león hambriento. Pero ya no vivimos en ese mundo. Kurzweil cree que en los próximos años se vivirá «un cambio tecnológico tan acelerado y profundo que representará una ruptura en el tejido de la historia de la humanidad». Dado el ritmo de cambio imparable y nuestro avance de los ordenadores del tamaño de un edificio a los iPhone en los últimos cuarenta años, ¿qué nos deparan los próximos cuarenta años? Sin duda, cosas mucho mejores y también potencialmente mucho más maléficas de lo que ninguno de nosotros es capaz de imaginar.

No estamos ante una sencilla historia binaria en la que hay que determinar si la tecnología es buena o mala, sino ante una historia de retornos acelerados. ¿Cómo

podemos velar por nuestra seguridad en un mundo que avanza a tal velocidad? Estamos construyendo una civilización sumamente interconectada pero, al mismo tiempo, tecnológicamente insegura. En otras palabras, estamos construyendo un mundo conectado para cometer toda suerte de delitos y plantear un abanico de amenazas a la seguridad. Las pruebas, cada vez más contundentes, demuestran estos peligros y nos presentan a una nueva clase de delincuentes de élite, terroristas y gobiernos extranjeros dispuestos a explotar estas tecnologías a su libre albedrío. ¿El resultado? Cada vez estamos más conectados, pero también somos más dependientes y vulnerables.

La singularidad de los delitos

En el pasado, delinquir era un asunto fácil. Cualquier aspirante a hacerlo sólo tenía que comprarse una navaja o una pistola, ocultarse en un callejón oscuro y asaltar por sorpresa a una víctima que se aproximara exigiéndole: «Dame todo lo que tengas». Aparte de ser una cuestión de una moralidad despreciable, los hurtos eran un modelo de negocio fantástico que había sobrevivido durante milenios. Los costes para arrancar la empresa eran bajos y los delincuentes podían fijar su propio horario laboral. Por supuesto, como cualquier empresario, bregaban con un problema evidente: cómo hacer crecer su negocio. Incluso un ladrón experto sólo podía robar a un determinado número de personas al día, cinco o seis a lo sumo, si le sonreía la suerte.

Sin embargo, afortunadamente, la tecnología proporcionó a los aspirantes a delincuentes una respuesta para sobreponerse a los problemas de escalabilidad que afrontaba su negocio, y dicha solución procedió de un lugar insospechado: la locomotora. Como es de suponer, cuando se inventaron los trenes nadie previó que podían verse sujetos a robos. En cambio, los delincuentes sí vieron en ellos una gran oportunidad y no perdieron el tiempo a la hora de aprovechar aquella nueva tecnología. Así, en lugar de robar a las personas de una en una, gracias a los trenes a vapor, hombres armados podían robar a doscientas o trescientas personas simultáneamente y ampliar con ello sobremanera las oportunidades de su negocio y sus beneficios.

Entre estos primeros delincuentes, Bill Miner, Jesse James y Butch Cassidy forjaron sus fortunas mediado el siglo XIX robando el cargamento de los trenes y el dinero y las joyas de los pasajeros[10]. Los asaltos a los trenes continuaron siendo una forma viable de empleo delictivo durante más de cien años, que culminó con el gran atraco a un tren en el Reino Unido en 1963, en el cual una banda de ladrones se apoderó de un convoy del Royal *Mail* que cubría el trayecto entre Glasgow y Londres. Su golpe planificado entregó a la banda de ladrones 2,6 millones de libras,

el equivalente a 46 millones de libras de hoy en día (o 7,28 y 76 millones de dólares, respectivamente[11]).

Si damos un salto hasta el presente, vemos que la delincuencia también puede beneficiarse enormemente de la naturaleza exponencial de la tecnología. Usando Internet, los ladrones han pasado de robar a personas sueltas o a centenares de ellas de manera simultánea a robar a miles y ahora incluso a millones. Como consecuencia, lo que estamos presenciando es un cambio de paradigma fundamental en la naturaleza de los delitos y en su comisión. Con la tecnología, los delitos aumentan, y lo hacen de modo exponencial.

Tal como se ha señalado previamente, el ataque contra T. J. Maxx de 2007 fue el delito al por menor más importante en su especie en aquel entonces y, en un principio, afectó a cuarenta y cinco millones de clientes y sus datos financieros. Sin embargo, los titulares de prensa dejaron claro por activa y por pasiva que el de TJX no era un incidente aislado. En junio de 2011, unos atacantes pusieron en jaque la red de juegos de Sony PlayStation y obtuvieron acceso a más de setenta y siete millones de cuentas en línea, que incluían los números de tarjeta de crédito, los nombres, las direcciones, las fechas de nacimiento y las credenciales de acceso a los juegos de las víctimas. El incidente hizo que la red de PlayStation permaneciera inactiva durante días y afectó a clientes de todo el mundo[12]. Los delincuentes no han perdido el tiempo a la hora de aprovechar los avances tecnológicos que hemos incorporado a nuestras vidas, incluidas las consolas de juego. Al final, los analistas financieros calcularon que la factura de reparación por el incidente de piratería que sufrió Sony PlayStation costó a la empresa más de mil millones de dólares en pérdida de negocios, asesores externos y demandas varias[13].

Tiempo después, en 2013, las tiendas de la cadena Target repartidas a lo ancho y largo de Estados Unidos admitieron que también habían sido víctimas de un ciberataque contra sus terminales de tarjetas de débito y crédito en los puntos de venta. El episodio no podía haberse producido en un momento peor para la empresa, en el punto álgido de la temporada de ventas navideñas. En aquel incidente se robaron datos de más de cien millones de cuentas, en un ataque al parecer ingeniado por un pirata informático de diecisiete años desde Rusia[14].

Imagina la envergadura y la enormidad de las pérdidas. Cerca de un tercio de la población estadounidense sufrió un robo de manera simultánea. Jamás antes en la historia de la humanidad había sido posible que una sola persona robara 110 millones de nada, por no mentar ya el robar a más de cien millones de personas de golpe.

Y por increíble que fuera el ataque contra Target en cuanto a dimensiones y alcance, poco después, en agosto de 2014, las cifras fueron sobrepasadas por un grupo de *hackers* rusos que sustrajeron 1200 millones de nombres de usuarios, contraseñas y otros datos confidenciales procedentes de 420 000 sitios web, según informó Hold Security[15]. La delincuencia también se ha internado en la era de la ley de Moore, y tiene consecuencias exponenciales para todos nosotros.

Controla el código y controlarás el mundo

> El progreso tecnológico es como un hacha en manos de un delincuente patológico.
>
> ALBERT EINSTEIN

Mientras la raza humana en su conjunto se conduce rumbo a una conexión ubicua en Internet, nos estamos transformando tanto a nosotros mismos como al mundo. Esta interconectividad global generará un bien tremendo. El hombre se vuelve cada vez más omnisciente a medida que cada hecho o pensamiento jamás registrado se pone a su disposición a tiempo real, al margen de cuál sea su fuente o ubicación. Desde las fórmulas químicas para la fotosíntesis hasta la temperatura actual en Bakú, quién ganó el torneo de críquet por condados ingleses en 1901 o las últimas travesuras de Justin Bieber, podemos saberlo todo con sólo conectarnos a ese cerebro global que es Internet.

Simultáneamente, el hombre también se vuelve más omnipotente a medida que los objetos del mundo se colocan en línea. Ahora puede activar su DVR desde la autopista y poner en marcha su coche desde el salón de casa. Las impresoras 3D imprimen piezas de automóviles y materiales de construcción. Bombas de insulina para diabéticos, marcapasos y desfibriladores cardiacos implantables están conectados a Internet y transmiten datos digitales vitales a los médicos en tiempo real. Hoy en día, los cirujanos incluso pueden realizar operaciones transatlánticas a través de sustitutos robóticos teleconectados, y dotar con ello de cirujanos a poblaciones donde ninguno de ellos ha puesto nunca el pie[16]. Los seres humanos tienen hoy la capacidad de controlar cosas al otro lado del planeta de modos que previamente se nos habrían antojado inimaginables e imposibles.

Pese a que existen ventajas evidentes en términos de costes, eficiencia y capacidad vinculadas con tales transformaciones, también es cierto que añaden una tremenda complejidad a nuestro mundo. Un aproximación muy burda para examinar tales complejidades estriba en tener en cuenta el número de líneas de código informático (LOC) necesarias para que funcione un sistema o un fragmento de *software* concreto. Por ejemplo, el Guidance Computer del *Apollo 11* de 1969 que guió a buen puerto a los astronautas durante los 356 000 kilómetros que separan la Tierra de la Luna, ida y vuelta, contenía sólo 145 000 LOC, una suma irrisoria y un logro asombroso medido según los estándares actuales[17]. A principios de la década de 1980, cuando la lanzadera espacial se puso en funcionamiento, su *software* de vuelo principal había aumentado a una cifra todavía relativamente magra de 400 000 LOC[18].

En comparación, Microsoft Office 2013 está formado por 45 millones de LOC, algo por debajo de los 50 millones de líneas de código necesarios para ejecutar el

Gran Colisionador de Hadrones ubicado en la Organización Europea para la Investigación Nuclear. En la actualidad, el *software* requerido para ejecutar los relojes de los automóviles ronda la nada desdeñable cifra de 100 millones de LOC, muy inferior a los 500 millones de LOC, una cantidad de líneas de código sin precedentes, que, según se informó, se requerían para ejecutar el tan difamado sitio web de la Seguridad Social del gobierno estadounidense: HealthCare.gov[19]. Si bien es difícil establecer comparaciones directas, HealthCare.gov era aproximadamente treinta y cinco veces más complejo que el sistema de guía que condujo al *Apollo 11* hasta la Luna y de regreso a la Tierra. Huelga preguntarse por qué el sitio web se colgó… y dejó de funcionar.

La complejidad creciente del *software* informático tiene consecuencias directas en materia de seguridad internacional, sobre todo a medida que los objetos físicos de los cuales dependemos, como son automóviles, aviones, puentes, túneles y dispositivos médicos que se implantan, se transforman en código informático. Cada vez más objetos físicos se convierten en tecnologías de la información. Los coches son «ordenadores en los que montamos» y los aviones no son más que «cajas Solaris voladoras acopladas a puñados de sistemas de control industriales»[20]. Y a medida que todo este código aumenta de tamaño y de complejidad, también lo hace el número de errores y fallos de *software*. De acuerdo con un estudio realizado por la Carnegie Mellon University, el *software* comercial tiene de promedio entre veinte y treinta errores por cada mil líneas de código, de manera que cincuenta millones de líneas de código equivalen a entre un millón y un millón y medio de errores potenciales que aprovechar[21]. Tal es la base de todos los ataques de *software* malicioso, que aprovechan estas vulnerabilidades para conseguir que el código efectúe algo imprevisto. Conforme el código informático se vuelve más elaborado, los llamados *bugs* de *software* se multiplican y la seguridad se pone en entredicho, con mayores consecuencias para el conjunto de la sociedad.

Las crecientes complejidades del sistema, incluso cuando no las aprovechan intencionadamente agentes malignos, pueden representar graves riesgos para la seguridad. Pongamos, por ejemplo, el apagón de la empresa eléctrica Northeast que en 2003 dejó a cincuenta y cinco millones de personas sin luz en Canadá y Estados Unidos durante días. Una red eléctrica laberíntica y un *bug* de *software* desembocaron en el mayor apagón de la historia de Norteamérica[22]. Los fallos informáticos también tuvieron un papel señalado en el desastre de 2010 de la plataforma petrolífera Deepwater Horizon, en el que once obreros fallecieron y el cual provocó la catástrofe ambiental más grave de la historia de Estados Unidos, con el vertido de 4,9 millones de barriles de petróleo en aguas del golfo de México[23]. En una audiencia gubernamental acerca del desastre, Michael Williams, el técnico en electrónica jefe de la plataforma Deepwater Horizon, testificó que los sistemas de monitorización y control de perforaciones cruciales quedaron paralizados por frecuentes fallos del *software* y antes de que la explosión hundiera la plataforma

petrolífera, una «pantalla muerta azul» cubrió el ordenador que la controlaba[24].

A pesar de que el apagón de Northeast de 2003 y el desastre de la Deepwater Horizon fueron sin lugar a dudas accidentes, permiten atisbar el tremendo daño que puede derivarse de un mal funcionamiento de los sistemas informáticos. No obstante, la única diferencia entre que un sistema informático falle por accidente o por una acción delictiva radica en la intencionalidad. Dado el gran número de *bugs* en el código informático actual, ¿qué podría llegar a ocurrir si se aprovecharan con fines viles? La misma tecnología que puede salvar el mundo y permitir la globalización puede caer en manos de radicales, criminales, terroristas y gobiernos que pretendan destruirlo.

Por desgracia, una vez se suelta una ciberarma en el ancho mundo, no se destruye, sino que puede utilizarse para otros objetivos. A diferencia de las bombas convencionales, que explotan en millones de fragmentos cuando impactan en sus objetivos, el *malware* puede utilizarse como arma de manera reiterada. Pese a que ejércitos y servicios de inteligencia inviertan millones de dólares secretamente en el desarrollo de un arma concreta, el código informático es fácil de copiar. Una vez publicado, queda a disposición de los *hacktivistas*, organizaciones delictivas y terroristas, quienes pueden explotarlo para sus propios fines, cosa que posibilita nuevas formas de proliferación de ciberarmas.

Imagina un cóctel Molotov virtual que, una vez arrojado, pudieran lanzar de vuelta desde el otro lado de las vallas. Ya hemos visto cómo esto sucedía cuando organizaciones delictivas y gobiernos corruptos han copiado diseños de código en un inicio utilizados contra ellos, los cuales han reconducido para perpetrar sus propios ataques[25]. Mientras el código informático continúe utilizándose como arma, los ataques de esta índole irán ganando en frecuencia y sofisticación.

Por desconcertante que resulte, lo cierto es que hasta la fecha no se ha creado ningún sistema informático que no pueda piratearse, un hecho que da que pensar, si tenemos en cuenta la confianza categórica que hemos depositado en estas máquinas para todo, desde la comunicación hasta el transporte pasando por la sanidad. No sólo son una farsa las contraseñas y las verificaciones del sistema que hicieron tan vulnerable a Mat Honan, sino también los programas informáticos que utilizamos para hacer funcionar el mundo. En una sola frase: cuando todo está conectado, todos somos vulnerables.

El poder de la ley de Moore no se aplica exclusivamente a los aspectos positivos de la tecnología, sino también a los negativos. Con la ley de Moore llegan las infracciones de la ley de Moore, perpetradas por delincuentes, terroristas, *hacktivistas* y agentes estatales que aprovechan las tecnologías a voluntad. Todos ellos son plenamente conscientes de cómo sacar partido a las complejidades de los sistemas y del *software* mal programado para obtener lo que desean de esta civilización fundamentada en la tecnología y con un desarrollo acelerado en la cual vivimos. A la par que todos los objetos se transforman en ordenadores y todos los ordenadores se

ejecutan con código, estos nuevos y poderosos agentes ilícitos han entendido claramente que, si se controla el código, se controla el mundo.

Ahora bien, no sólo tenemos que preocuparnos de los delincuentes y de los gobiernos corruptos. A menudo, las mismas empresas y organizaciones a las que acudimos en busca de protección, consejo o entretenimiento nos dejan expuestos y completamente vulnerables, pues ellas también controlan el código que rige el funcionamiento de nuestras vidas.

Capítulo 4

No eres el cliente, eres el producto

La verdad te hará libre, pero antes te pondrá de mala leche.

GLORIA STEINEM

El Parkinson, la esclerosis múltiple recidivante, la fascitis necrotizante, la leucemia linfoblástica aguda, la diabetes juvenil, el VIH, la esclerosis lateral amiotrófica (ELA)… recibir un diagnóstico de cualquiera de estas enfermedades supone un mazazo para cualquier persona, una noticia que le cambia la vida para siempre. En el pasado, las personas con enfermedades como éstas habrían quedado sumidas en la depresión y se habrían sentido solas, incapaces de hablar de su problema con otras personas que entendieran exactamente por lo que estaban pasando. Es más, la escasez de información médica comprensible escrita para seres humanos normales y corrientes habría aislado a estos pacientes de sus amistades y familiares. Eso fue lo que llevó a Jamie y Ben Heywood (a cuyo hermano diagnosticaron ELA) a fundar el sitio web en Internet PatientsLikeMe.com, con el fin de permitir a los visitantes compartir sus historias y conectar con otras personas que padecieran los mismos problemas de salud. Desde su fundación en 2004, el sitio web se ha convertido en una comunidad integrada por más de 200 000 pacientes diagnosticados con mil quinientas enfermedades únicas[1]. Para miles de personas, PatientsLikeMe.com ha sido una tabla de salvación tanto en el sentido figurado como en el literal, pues ha permitido a los usuarios ampliar conocimientos acerca de sus afecciones e intercambiar estrategias de supervivencia y protocolos de tratamiento mediante diversos foros de debate en línea.

Fue precisamente esa oportunidad de conectar con otras personas lo que llevó inicialmente a consultar el sitio web a Bilal Ahmed, un empresario de treinta y tres años de edad residente en Sídney, Australia. Ahmed sufría de ansiedad y depresión desde la muerte de su madre, y le resultaba difícil hablar de su problema con sus amistades y familiares[2]. Ahmed creó una cuenta con un seudónimo en PatientsLikeMe y se unió a su Mood Forum, el foro de estados de ánimo donde los usuarios comparten detalles íntimos acerca de trastornos emocionales como bipolaridad, trastorno por estrés postraumático (TEPT), bulimia, adicciones, trastorno obsesivo-compulsivo y pensamientos suicidas. En el Mood Forum, Ahmed enumeró debidamente sus síntomas, los resultados de sus análisis y todos los medicamentos que le habían prescrito para tratarle la depresión. Allí conectó con otros pacientes de todo el mundo, entabló amistades y compartió los detalles más íntimos relativos a su

enfermedad en el sitio web protegido por contraseña, donde obtuvo justamente el tipo de apoyo que tanto había anhelado.

Y por ese mismo motivo fue por lo que Ahmed se sintió tan ultrajado cuando PatientsLikeMe le informó de que se habían producido «actividades no autorizadas» en su tablón de debate en Mood Forum. A la una de la madrugada del 7 de mayo de 2010, los administradores del sistema notaron una actividad sospechosa procedente de varias cuentas nuevas que estaban «rascando» o, lo que es lo mismo, copiando todos y cada uno de los mensajes del foro en línea privado y descargando la información a un sitio web externo. PatientsLikeMe acabó identificando al intruso responsable de aquella infracción: la empresa Nielsen, el mismo gigante de la publicidad conocido por hacer estadísticas de audiencia para la televisión estadounidense. Una filial de Nielsen conocida como BuzzMetrics admitió haber sustraído los datos, que añadió a su compilación de información en línea hurtada a otros 130 millones de blogs, ocho mil tablones de mensajes, Twitter, Facebook y otras redes sociales que rastreaba. Nielsen vende estos datos a anunciantes, comerciantes y, en este caso, a las principales farmacéuticas como materia prima de una industria de minería de datos mundial que mueve varios miles de millones de dólares en volumen de negocios.

La indignante actividad de Nielsen, pese a ser repugnante en términos éticos, era técnicamente legal de acuerdo con la actual ley federal y, el 18 de mayo de 2010, PatientsLikeMe reveló el incidente a toda su comunidad de usuarios. La empresa aprovechó la oportunidad para recordar a sus usuarios sus propios términos y condiciones en política de privacidad:

> Tomamos la información que pacientes como usted comparten acerca de su vivencia de la enfermedad y la vendemos a nuestros socios (es decir, empresas que desarrollan o venden productos a los pacientes). Estos productos puede incluir medicamentos, dispositivos, equipamiento, seguros y servicios médicos. […] Cualquier información que comparta (aunque no se visualice en el momento presente) podrá ser compartida[3].

Alto, ¿qué? La nota que revelaba la intromisión de Nielsen ya era bastante mala, pero el mensaje de correo electrónico que la siguió, en el que el sitio web detallaba su política de privacidad, hizo que los usuarios de PatientsLikeMe despertaran de golpe. La mayoría de ellos cayeron por primera vez en la cuenta de que toda la información médica que previamente habría permanecido guardada a buen recaudo en el archivador de la consulta de su médico —desde su enfermedad, hasta la fecha de su diagnóstico, su historial familiar, los síntomas, el recuento de CD4, las cargas víricas, los resultados de los laboratorios, su información geográfica, su sexo, edad, fotografías y secuencias genéticas enteras—, estaba siendo vendida por PatientsLikeMe, el mismísimo lugar al que, desesperados, habían acudido para buscar ayuda y en el cual habían confiado para salvaguardar su información[4].

Pese a que PatientsLikeMe afirmaba que sólo vendía datos anónimos y

despersonalizados de sus pacientes, empresas de datos nuevas y emergentes como PeekYou LLC, en Nueva York, hacía tiempo que habían inventado una variedad de técnicas patentadas que permiten emparejar los nombres reales de las personas con los seudónimos que utilizan en blogs, chats y Twitter. En otras palabras, cualquier empresa farmacéutica o mutua de salud que quisiera obtener la información de PatientsLikeMe únicamente tenía que contratar a PeekYou para que, mediante ingeniería inversa, emparejara en masa los nombres de usuario o seudónimos con los datos de identificación personal. Para Bilal Ahmed, aquello significaba que todos los datos personales que había aportado en PatientsLikeMe ahora eran propiedad de Nielsen/BuzzMetrics. En una entrevista pública concedida tras su identificación, Ahmed comentó que se había sentido ultrajado por el incidente y había procedido a borrar de inmediato todas sus publicaciones en el sitio web, así como el listado de medicamentos que le habían recetado, pero para entonces ya era demasiado tarde[5]. Cada vez que él u otros pacientes habían publicado informes con todo lujo de detalle acerca de sus enfermedades y síntomas en PatientsLikeMe, había empresas como Nielsen acechando en segundo plano para sustraer todos los datos que compartían. Y aquellos que no habían sido hurtados por terceras partes, PatientsLikeMe los había vendido libremente, tal como enunciaban en su política de privacidad en letra pequeña que ni Ahmed ni muchos otros habían leído al crear sus cuentas.

Como bien descubrió Ahmed, las redes sociales son los nuevos registros públicos. Todo lo que se comparte en ellas, de manera voluntaria o involuntaria, es filtrado, clasificado y almacenado por los nuevos mastodontes de gestión de datos mundiales, que luego lo venden a anunciantes, gobiernos y agentes intermediarios de datos externos, todos ellos con un apetito voraz por conocer los detalles más íntimos de tu vida. Estos datos pueden utilizarse para determinar si uno padece enfermedades anteriores, si debe pagar una cuota más elevada por su mutua médica o si obtiene un empleo o una promoción laboral o no. Pese a que compartir tales datos puede ayudar, también puede acarrear el pago de una prima más alta por un seguro médico. Como consecuencia, los cientos de miles de personas que utilizaban PatientsLikeMe aprendieron una lección valiosa aunque también dolorosa: no somos los clientes de los sitios web, sino el producto, vendido al mejor postor en un esfuerzo por incrementar los beneficios de la empresa.

Un mundo cada vez más digitalizado: lo que no nos cuentan

En 2013, los estadounidenses pasaban más de cinco horas al día conectados a Internet con sus dispositivos digitales[6]. Leemos la noticias en sitios web administrados por la

CNN, el *New York Times* y ESPN. Comprobamos nuestros extractos bancarios en Citibank y Wells Fargo. Compramos en Amazon y Zara. Pagamos las facturas de electricidad y gas, concertamos visitas con el médico y comprobamos nuestro seguro sanitario con Blue *Cross*. Vemos *House of Cards* en Netflix y *Downton Abbey* en Hulu. Y eso no es más que el principio. Haz un alto un instante para pensar con qué fin has utilizado el *smartphone* hoy. El ochenta por ciento de nosotros comprobamos si tenemos mensajes nuevos transcurridos menos de quince minutos desde que nos despertamos[7]. ¿Has actualizado tu estado para informar a tus amigos de Facebook? Probablemente recibas un par de «Me gusta» o un comentario ingenioso de alguien. ¿Y qué hay de los autorretratos que le has enviado a tu pareja? Internet se ha convertido en una cueva del tesoro de información y entretenimiento inmensa y gratuita, y nos asomamos a la entrada con voracidad, como se espera de nosotros. Pero con cada paso que damos dejamos atrás a diario un rastro digital colectivo y trillado lo bastante grande como para llenar varias veces la Biblioteca del Congreso estadounidense. Cómo se crean, almacenan, analizan y venden estos datos son detalles que la mayoría de nosotros pasamos por alto, a nuestra cuenta y riesgo.

Nadie niega el poder de las redes sociales. En poco más de diez años desde su creación en 2004, Facebook ha pasado de tener cero suscriptores a 1300 millones de usuarios en todo el planeta, todo un acelerón[8]. Cada día se publican más de 350 millones de fotografías y el omnipresente botón de «Me gusta» se pulsa en torno a seis mil millones de veces[9]. Las redes sociales informan de nuestras citas, graduaciones, compras caseras, nacimientos, nuevas mascotas, matrimonios y divorcios. También pueden proveer instrumentos que propicien el cambio geopolítico, tal como vimos durante la Primavera Árabe de 2010, cuando un ejecutivo de Google llamado Wael Ghonim creó una página de Facebook para informar de la matanza de un joven manifestante egipcio a manos de las fuerzas de seguridad internas de Hosni Mubarak. «Dos minutos después de publicar su página en Facebook, tenía 300 suscriptores. Tres meses después, esa cifra había ascendido a más de 250 000[10]». En la misma línea, Twitter, Google y otros servicios se anotaron el crédito de ayudar a impulsar el cambio en Túnez, Irán y Libia. Y si bien la historia juzgará el papel que las redes sociales desempeñaron en la Primavera Árabe, no cabe ninguna duda de que estos servicios pueden ser una fuerza impulsora del bien.

El atractivo de estas herramientas es evidente. Al fin y al cabo, la mayoría de nosotros nos pasamos la vida merodeando por la web en busca de música, recetas, consejo para realizar inversiones, noticias, indicaciones, oportunidades de negocio, cotilleos sobre famosos y resultados deportivos. Cuando no estamos comprobando el correo electrónico, andamos jugando a *Temple Run* o *Fruit Ninja*. Y todo ello gratis. Incluso las tasas que otrora pagábamos a las agencias de viajes, diarios y discográficas han desaparecido, eliminadas gracias a las generosas personas que pusieron a nuestro alcance la World Wide Web. Pero ¿alguna vez te has detenido a preguntarte por qué Google nunca te envía una factura?

Pregunta a cualquiera por qué Google, Facebook, Twitter, YouTube y LinkedIn son gratuitos y comprobarás que te responde con vaguedades. Muchos creen que es gracias a la publicidad, o sea, a esos molestos anuncios o pantallas desplegables con los que nos bombardean sin cesar. Y quizá sea cierto, pero eso sólo es una pequeña parte de la historia. Otros creen que la compensación es harto sencilla: estas empresas nos ofrecen valiosos servicios de manera gratuita, como correo electrónico, noticias, vídeos y un lugar para publicar fotografías y, a cambio, les aportamos un poco de información sobre nosotros mismos. De vez en cuando tenemos que ver un anuncio diseñado específicamente con acuerdo a nuestras necesidades, pero los ajustes de seguridad nos ponen al mando del timón y nadie resulta herido, ¿no es así? Ojalá fuera tan simple. La realidad del trato que hemos hecho con ellas es mucho más desconcertante.

Pongamos por ejemplo a Google, una empresa fundada en 1998 por dos estudiantes de doctorado de la Universidad de Stanford, Larry Page y Serguéi Brin en el garaje de un amigo en Menlo Park, California. La pareja inventó un algoritmo rompedor que mejoraba sobremanera los resultados de las búsquedas en la aún incipiente World Wide Web y sedujo a una legión de seguidores fieles, atraídos por su sencilla interfaz y la alta calidad de los resultados de búsqueda. En 2000 empezaron a vender palabras clave para anuncios publicitarios de productos particulares alineados con frases de búsqueda determinadas. Por ejemplo, si se busca «París, Francia», aparecerá una barra lateral con anuncios de Air France, empresas de seguros de viajes y hoteles Hilton. Las empresas que buscaban nuevos clientes pudieron así utilizar las palabras clave de los anuncios de Google con una precisión hasta entonces desconocida y obtenían unos resultados mucho más satisfactorios por el capital invertido en publicidad. Lo que surgió como una idea humilde de dos alumnos de Stanford en 1998, en 2015 se había convertido ya en un gigante mundial.

Con el transcurso de los años, Google ha presentado docenas de productos que hacen nuestras vidas más sencillas y productivas. Cuando lanzó Gmail en 2004, ofrecía 1 GB de datos, un espacio asombroso que superaba con creces los irrisorios 200 MB que ofrecía el proveedor de correo electrónico más importante del momento, Hotmail, de Microsoft. Y a medida que la joven empresa avanzaba a pasos agigantados, surgieron otros productos maravillosos y finalmente conocimos Google Calendar, Google Contacts, Google Maps, Google Earth, Google Voice, Google Docs, Google Street View, Google Translate, Google Drive, Google Photos (Picasa), Google Video (YouTube), Google Chrome, Google+ y Google Android, por mencionar unos cuantos. Uno a uno, servicios como las llamadas telefónicas, traducción, mapas y procesamiento de texto, servicios por los que previamente pagábamos cientos de dólares (piénsese en el Office de Microsoft), pasaron a ser gratuitos.

La interpretación más benévola de este mundo de la abundancia sería que Google se limitaba a proporcionar los productos que el público demandaba y satisfacía

nuestras necesidades tecnológicas crecientes (y las de los anunciantes). Una explicación menos altruista podría ser que cada uno de los productos mencionados se creó con la intención específica de engañar, engatusar y convencer a los usuarios de revelar un volumen creciente de datos acerca de sí mismos y de sus vidas *ad infinitum*. La población tal vez se opusiera si comprendiera de verdad la auténtica naturaleza del intercambio. Así que, parafraseando a Otto von Bismarck, es mejor para los clientes de Google no ver ni saber cómo se elabora la salchicha. Sin embargo, descorrer el telón y analizar la fábrica de salchichas es fundamental para entender la montaña creciente de riesgos en materia de seguridad de los datos que afronta el mundo actual.

El desvío gradual de nuestros datos se inició de manera cándida cuando empezamos a utilizar Google para efectuar búsquedas en Internet. Google rastrea y registra todas las búsquedas, así como todos los enlaces en los que se clica. A partir de ese producto de búsqueda inicial, la adquisición cuidadosamente orquestada de los datos personales se lleva a cabo con una precisión ingeniosa. Con el tiempo, el motor de búsqueda dejó de ser suficiente y Google se dispuso a hallar nuevos modos de obtener datos acerca de sus usuarios, de sus esperanzas, sueños y deseos. ¿El resultado? Gmail. Al proporcionar una enorme cantidad de espacio de almacenamiento y una experiencia maravillosamente fluida, Google obtuvo acceso tanto a tus mensajes de correo electrónico personales como profesionales. De este modo, Google no sólo conocía tus búsquedas, sino todo lo que escribías y a quién. Google escaneó y leyó electrónicamente tus mensajes y halló nueva información privilegiada que podía ofrecer a sus anunciantes, aumentando con ello las tarifas a medida que refinaba el perfil de sus usuarios. Así, si le enviabas un correo a tu madre diciéndole que estabas triste por una ruptura reciente, Google podía sugerirte un antidepresivo, entradas para el Club de la Comedia o unas vacaciones en el Caribe. Siempre que la sesión permaneciera abierta en Gmail, la aplicación podía rastrear todas tus búsquedas con tu identificador único en la empresa; como resultado de ello, el perfil que Google tenía de cada usuario se volvía cada vez más rico, al igual que la empresa.

Cuando Google ofreció a los usuarios la oportunidad de guardar sus contactos en línea, pudo a su vez evaluar el tamaño, la fuerza y el poder adquisitivo de su red social. Y cuando Google introdujo su programa de mapas, Maps, y proporcionó indicaciones para conducir y GPS de manera gratuita, tuvo acceso a conocer los lugares a los que iba cada cual. Google se preguntaba a quién llamaría cada usuario por teléfono, y para saberlo creó Google Voice. De este modo, no sólo pudo realizar el seguimiento de todas y cada una de las llamadas telefónicas de cada usuario, sino que, además, tuvo ocasión de transcribir los mensajes del buzón de voz utilizando *software* de reconocimiento y transcripción de voz. Además de ser un hito técnico maravilloso en la fecha de su creación, Google Voice permitió a Google saber de qué hablaba cada usuario con sus interlocutores. Si alguien, por ejemplo, te dejaba un

mensaje en el buzón de voz sugiriéndote que cenaras comida italiana, Google podía vender esa información a sus anunciantes y, de repente, tu mundo personal de Google estaría repleto de anuncios de *pizza*. Para mayor precisión, Google creó el sistema operativo (OS) Android y lo regaló a sus usuarios. A cambio, Google tenía la oportunidad de seguirlos allá donde se llevaran el *smartphone*.

Por supuesto, si Google informara a sus usuarios de todo esto, se asustarían, de manera que, para que eso no ocurriera, concibió una magnífica estratagema, una especie de hoja de parra. En el momento de su fundación, Google se protegió vendiéndose como el supuesto perdedor, el pobre hombre que batallaba contra el gigante Microsoft. De hecho, Google se presentó a sus usuarios como el bueno de la película, hasta tal punto que decidió convertir la frase «No seas malo» en el lema oficial de la empresa. Y para apaciguar las posibles dudas residuales, crearon unos iconos y unos gráficos tan «monos», como el infantil logotipo de colores de Google o el adorable marcianito verde de Android, que no suscitaban ninguna sensación de amenaza y, en cambio, sí invitaban a confiar en ellos. Google Doodles, los dibujos en la página de inicio que rinden tributo a cualquiera desde Martin Luther King hasta Gandhi, acabaron por tranquilizar al público: aquellos tipos eran buena gente. Además, Google implementaba políticas de privacidad serias para protegernos, ¿no es cierto? Echemos el freno.

Mirado con ojo crítico, Google crea sus productos no para ofrecernos correo electrónico gratuito, sino para obtener cada vez más datos de cada uno de nosotros. Como un camello que sostiene la primera papelina de heroína ante un futuro yonqui, Google nos regaló algo «pagando la casa» y fue luego cuando nos dimos cuentas de las implicaciones del trato que estábamos haciendo. Pero para entonces ya era demasiado tarde. Ello quedó claro cuando, a principios de 2012, Google anunció que iba a fusionar los datos de sus setenta productos y servicios. El resultado: una imagen unificada, profunda y sin precedentes de cada uno de los usuarios y de su mundo personal. Hasta entonces, las búsquedas que habías efectuado en Google, lo que hacías en tu teléfono Android y los vídeos que veías en YouTube eran datos que, *en teoría*, Google almacenaba por separado. Pero la cosa cambió a partir de aquel momento y ahora Google cuenta con una imagen única, unificada y muy detallada de ti y de todo lo que haces en el Googleverso[11]. Hay quien afirma, incluso, que Google te conoce mejor que tú mismo. Y precisamente por disponer de todos esos datos puede exigir las máximas tarifas a los anunciantes por la información personal de sus usuarios.

Por si no había quedado ya bastante claro, tú no eres el cliente de Google, eres su producto. Por eso no recibes ninguna factura. Pero eso no existe ningún teléfono gratuito para solicitar asistencia técnica. Estos servicios se reservan para sus verdaderos clientes: los anunciantes que adquieren todos los datos que vas dejando por la superautopista de la información de Google. Tú eres la mercancía que Google vende a otras personas; ése es el trato que nunca ha quedado claro y, tanto si eres

consciente de ello como si no, eres cómplice de este proceso.

Cabe decir en su favor que Google proporciona productos maravillosos para satisfacer las necesidades de sus usuarios y que la empresa cuenta con un personal formado por montones de empleados con gran talento consagrados a su trabajo. Pero no te equivoques: su lealtad estará siempre, principalmente, con sus anunciantes, que son quienes pagan las facturas, y con sus accionistas, con los cuales tiene una obligación fiduciaria de extraer de ti (mediante sus productos y su cadena de provisiones) el máximo valor posible. Por eso Google almacena cada búsqueda que has realizado en su sitio web de manera indefinida: «conservadores en el gobierno de Madrid», preguntaste hace unos diez años; «síntomas de la gonorrea», escribiste tras una relación esporádica; «vídeos de Girls Gone Wild», consultaste mientras te dirigías a trabajar en un hotel, o «¿es mi esposo gay?», buscaste en una ocasión en que te sentías alicaída y sola[12].

Google no olvida y Google no borra. Cada una de las preguntas anteriores sirve para crear un perfil de usuario, para categorizarlo y venderlo a los anunciantes y las empresas de minería de datos, que realizan asunciones adicionales con relación a cada usuario en función de sus búsquedas, mensajes de correo electrónico, mensajes en el buzón de voz, fotografías, vídeos y ubicaciones catalogadas por Google. ¿Cuántos datos procesa Google a diario?, te preguntarás. Cerca de 24 petabytes (es decir, un millón de gigabytes o 1000 terabytes, una medida utilizada para describir el volumen de datos). Para ponerlo en perspectiva, se necesita aproximadamente «un gigabyte de datos para almacenar diez metros de libros en un estante»[13]. Si todos los datos de Google procesados a diario se imprimieran y esos libros se apilaran uno encima de otro, la pila llegaría a medio camino entre la Tierra y la Luna. Tal es la cantidad de información que Google almacena acerca de sus usuarios… ¡cada día!

Todos estos datos proporcionan una información privilegiada colosal y un poder tremendo, pero, como dice el dicho: el poder corrompe. En todo el mundo, Google ha tenido que afrontar demandas reiteradas por infracciones de la privacidad, fallos de seguridad, uso indebido de datos de los usuarios, robo de propiedad intelectual, evasión de impuestos y contravenciones a las leyes antimonopolio[14]. Después de una demanda presentada por treinta y ocho fiscales generales estatales estadounidenses en 2013, Google admitió que sus estrafalarios coches Street View, dotados con cámaras panorámicas de 360 grados y alta tecnología en el techo, no sólo tomaban fotos para su producto de mapas Street View mientras transitaban por las calles de nuestros vecindarios, sino que, además, robaban datos de los ordenadores guardados en nuestros hogares y oficinas, inclusive contraseñas, mensajes de correo electrónico, fotografías, mensajes de chat y otra información personal de usuarios informáticos desprevenidos[15].

En octubre de 2013, un juez federal rehusó desestimar una demanda colectiva contra Google alegando que su práctica de leer y escanear las cuentas de Gmail de los usuarios infringía las leyes estadounidenses contra los teléfonos intervenidos y las

escuchas ilegales[16]. Antes de eso, en 2012, Google tuvo que pagar una multa récord de 22,5 millones de dólares impuesta por la Comisión Federal de Comercio cuando se reveló que eludía de manera rutinaria la configuración de privacidad de los ordenadores Apple y de los usuarios del navegador web de Apple Safari con la finalidad de seguir los movimientos de dichos usuarios por Internet en contra de sus deseos claramente especificados.

Sin lugar a dudas, Google es una de las empresas más innovadoras y, en su intento por persuadirte porque cada vez le facilites más información para sus clientes reales (los anunciantes), tiene previsto lanzar una serie de productos nuevos que harán que las preocupaciones del pasado con respecto a la privacidad empalidezcan en comparación con las futuras. Uno de dichos productos es Google Glass, un ordenador ponible con forma de gafas con una «pantalla óptica que se monta en la cabeza», se conecta a Internet y es capaz de proyectar información visual en una pantalla incrustada en las gafas. El dispositivo funciona con el sistema operativo Android y permite fotografiar, grabar vídeo y reproducirlo a tiempo real mediante su cámara y su micrófono incorporados.

A principios del año 2014, el dispositivo Google Glass protagonizó un episodio de *Los Simpson* titulado «Gafas y la ciudad», en el que se entregaba a todos los empleados del señor Burns un par de «Oogle Goggles»[17]. En el capítulo, Homer Simpson y sus colegas utilizan las gafas para obtener información nueva acerca de las personas y las cosas que los rodean. En lo que supone un mal presagio, o quizá un momento clarividente, el señor Burns, sentado en el centro de mandos que es su oficina, es capaz de acceder a las gafas de todos sus empleados y averiguar qué ven y hacen en tiempo real (su objetivo es reducir el hurto de material de oficina).

Incluso el exdirector del Departamento de Seguridad Nacional de Estados Unidos (DHS en sus siglas en inglés) estadounidense, Michael Chertoff, ha explicitado su preocupación en cuanto a políticas públicas y privacidad con respecto a Google Glass[18]. Con buen criterio, Chertoff preguntó a quién pertenecían los derechos de los datos de los vídeos de los usuarios y si se minaría y analizaría toda la base de datos de vídeos con fines comerciales. También sería legítimo preguntarse qué acceso tendrá el gobierno a dichos datos, tanto de manera retrospectiva como en tiempo real, por motivos que pueden abarcar desde la lucha contra la delincuencia hasta la «seguridad nacional». Piensa en las implicaciones por un instante: al utilizar Google Glass, le entregas a la empresa el derecho a captar todos los momentos de tu vida diaria que retransmites en tiempo real, todo lo que ves y escuchas, para que pueda venderlos a sus anunciantes. ¿De verdad es eso lo que quieres? Por ejemplo, si, pongamos por caso, llevaras las gafas mientras te preparases el café de la mañana en albornoz, el algoritmo de visión de Google Glass identificaría que el objeto en tu campo de visión es una cafetera (algo más que plausible) y podría empezar a mostrarte cupones de descuento para las cafeterías Starbucks en la pantalla de las gafas. Dadas las transgresiones de la privacidad mencionadas con anterioridad con

respecto a este buscador gigante, ¿de qué más será capaz cuando nos adentremos en la era de la vigilancia portable?

La red social y su inventario: tú

Lógicamente, Google no es el único agente en este modelo de negocio de venderte a sus anunciantes: hay miles de empresas alrededor del mundo que se dedican a hacer lo mismo, la más destacada de ellas Facebook. Fundado por Mark Zuckerberg en su dormitorio en Harvard en 2004, Facebook es una historia de éxito icónica del Silicon Valley. Con más de 1200 millones de usuarios activos mundiales, Facebook es de lejos la mayor red social que existe en el mundo[19]. Su éxito ha consistido en permitir a la gente hablar de sí misma de modos previamente inimaginables. Orientación sexual, situación sentimental, escuelas donde se estudió, árbol genealógico, listas de amigos, edad, género, direcciones de correo electrónico, lugar de nacimiento, intereses informativos, historia laboral, catálogos de cosas favoritas, religión, afiliación política, compras, fotografías y vídeos: Facebook es el sueño de cualquier comerciante. Los anunciantes conocen hasta el último detalle acerca de la vida del usuario de Facebook, cosa que les permite ofrecerle productos con una precisión extrema en función del gráfico social que la red social ha generado.

Más aún, Facebook creó una serie de innovaciones que le permiten hacer el seguimiento de sus usuarios por toda la web, gracias a su omnipresente botón de «Me gusta». Te han entrenado para que hagas clic en esos pequeños botones azules con un pulgar optimista y expreses así tu apoyo a una idea, a una actualización de estado o a una fotografía; al fin y al cabo, es cuestión de educación. Tus amigos entienden que estás de acuerdo con su mensaje, pero lo que no veis ninguno es qué ocurre con los datos generados con cada uno de esos «Me gusta»: los datos se registran, diseccionan y se venden a comerciantes y agentes intermediarios de datos de todo el mundo. Cuando utilizas las ubicuas credenciales de inicio de sesión de Facebook para visitar sitios en Internet, como Spotify y Pandora, el motor de minería de datos de Facebook descifra que prefieres a Lady Gaga frente a Blake Shelton, del mismo modo que rastrea todos los sitios web que visitas que incorporan el icono de Facebook (incluso aunque no hayas iniciado sesión).

Por si no estuvieras compartiendo ya bastantes cosas, Facebook crea a su antojo nuevas reglas y regulaciones para obligarte a compartir más, como hizo en 2012, cuando instituyó su «función» obligatoria de la cronología. Aquel cambio proporcionó a los anunciantes una ventana dinámica y constantemente actualizada para asomarse a tus intereses vitales en cualquier momento, además de proveer más pienso a Facebook para venderles. Facebook, como Google, se ha criticado por activa y por pasiva por cuestiones relacionadas con la privacidad, la seguridad infantil y el

discurso del odio. Además, ha afrontado demandas judiciales en todo el mundo, la más reciente en las cortes federales estadounidenses de San José, California, por «interceptar de manera habitual y sistemática los mensajes privados de los usuarios […] y compartir los datos con los anunciantes y comerciantes»[20].

Y, por descontado, Google y Facebook no están solos en esta aventura de persuadirte para que reveles datos personales para luego venderlos: los acompañan Twitter, Instagram, Pinterest y centenares de empresas adicionales. Por ejemplo, ¿sabes que cada vez que le formulas una pregunta al agente de inteligencia artificial de Apple, Siri, la empresa graba tu voz y analiza y guarda la grabación como mínimo dos años[21]? Ahora bien, lo importante no es quién almacena tus datos, ya que todo el mundo parece estar haciéndolo en la actualidad, sino qué se hace con esa información. Si este pacto de Fausto fuera tan sencillo como proporcionarte servicios estimulantes «gratuitos» a cambio de unos cuantos datos, el mundo sería de color de rosa. Sucede que las cosas no son tan sencillas como parecen, ya que, como comprobarás en breve, conservar y almacenar estos volúmenes masivos de datos en un mundo tan conectado, dependiente y vulnerable te pone en riesgo de modos que posiblemente nunca hayas imaginado.

Filtras información, pero ¿cómo se las apañan para conseguirla?

Cada vez que visitas un sitio web, éste instala en el disco duro de tu ordenador o teléfono móvil unos archivos digitales invisibles llamados *cookies* que actúan a modo de marcadores. Con estos diminutos archivos informáticos es posible rastrear tus actividades por toda la Red. Además, todos tus dispositivos electrónicos tienen unas huellas únicas que permiten seguirte, ocultarte y catalogarte. Los identificadores únicos, como la dirección del protocolo de Internet (IP) de la red informática que usas para conectarte a Internet, el número de control de acceso a contenido (dirección MAC) de tus tarjetas de red Wi-Fi y el número IMEI o IMSI de tu teléfono móvil permiten a las empresas en línea saber exactamente qué dispositivos (y usuarios) utilizan sus servicios.

Todos estos datos se rastrean, unifican y explotan para ofrecer a las empresas en Internet y sus anunciantes una imagen clara y persistente de quién eres y cuáles son las actividades que efectúas en Internet. De acuerdo con un estudio realizado en 2012 por *Wall Street Journal*, uno de los negocios que más proliferan actualmente es el espionaje de internautas. En su informe, el diario destacaba cincuenta de los sitios web más populares y revelaba que, de promedio, cada uno de ellos dejaba más de 64 archivos de seguimiento en forma de *cookies* para que los anunciantes pudieran

rastrear y supervisar tus actividades en línea. El sitio web con más *software* de rastreo era Dictionary.com, que implantaba un total de 234 archivos de seguimiento en tu ordenador cada vez que lo visitabas[22]. Todas estas *cookies* que permiten rastrearte se combinan con tus «Me gusta», toques y tuits para brindar una imagen siniestramente detallada de tu yo digital. Podría decirse que estas «galletas» que se instalan en tu ordenador se transforman en monstruos de las galletas y revelan datos de ti que no tenías intención de hacer públicos.

Pero no sólo tú filtras datos acerca de ti a través de tus actividades en las redes sociales, sino que tus amigos y familiares también lo hacen. Cada vez que un amigo introduce tu nombre y dirección en sus contactos de Google o iPhone, proporciona a Google y a Apple tus datos personales. Si grabas la fecha de cumpleaños de tu sobrino, novia o de un colega de trabajo en el calendario de Outlook, Microsoft conocerá la fecha de nacimiento de esa persona. Y cuando tus amigos te etiquetan en una fiesta en Facebook (después de que hayas telefoneado a la oficina para decir que te encuentras mal y no irás a trabajar), comparten tu ubicación con los anunciantes y, potencialmente, con el resto del mundo, incluido tu jefe. A las redes sociales y a las empresas que operan en Internet les encanta que sus usuarios trabajen para ellas; es como tener monos de código libre rellenando informe tras informe y alimentando su gran máquina tragadatos.

Esto sucede incluso cuando tu amigo utiliza un sitio web o servicio de Internet concreto que tú no usas. Por ejemplo, si alguien no tiene una cuenta con Gmail, pero sus amigos sí, cuando envía un mensaje de correo electrónico a cualquiera de los 245 millones de usuarios de Gmail, Google se convierte en parte de su conversación. De manera que, si utilizas la dirección de correo electrónico de tu universidad o trabajo para enviarle a tu hermana un mensaje a su cuenta de Gmail, pese a que nunca hayas abierto una cuenta de Google en persona, Google leerá, escaneará y buscará en el mensaje palabras de interés que pueda vender a sus anunciantes, una práctica por la que ahora afronta una demanda en los tribunales federales[23]. En los alegatos de su defensa por la demanda presentada ante la juez Lucy Koh, Google afirmó, para pasmo del personal, que «nadie puede esperar legítimamente que se trate con confidencialidad la información que proporciona de manera voluntaria a terceras partes»[24]. En otras palabras, el argumento de Google es que, al enviar un mensaje de correo electrónico a cualquier usuario de Gmail, automáticamente cedes tus derechos de privacidad y consientes que tu mensaje y su contenido sea secuestrado y vendido, por mucho que se tratara de un mensaje privado y que ni siquiera tengas una cuenta con Gmail.

Pero no sólo tus amigos filtran datos sobre ti a terceras partes como Google, sino que también lo hacen tus hijos[25]. De hecho, los sitios web destinados a niños instalan más tecnologías de rastreo en los ordenadores que los sitios web para adultos. Pese a que una ley federal estadounidense titulada Children’s Online Privacy Protection Act (Ley de protección de la privacidad de los niños en Internet) limita la

información que los comerciantes online pueden recabar sobre los menores de trece años, esa norma se transgrede descaradamente de manera rutinaria. A los pequeños les presentan multitud de pantallas en las que les solicitan que se apunten a concursos, juegos y que rellenen cuestionarios, en un intento por obtener más datos acerca de ellos, contraviniendo las leyes federales. Empresas conocidísimas como McDonald's, General Mills, Viacom, Turner Broadcasting System y Subway han sido multadas por convencer a los niños de facilitarles datos en sus sitios web repletos de dibujos animados, como HappyMeal.com, ReesesPuffs.com, Nick.com y SubwayKids.com[26]. En otro caso, Sony BMG Music solicitaba a los menores que especificaran su dirección postal y sus número telefónicos en las páginas de fans de sus grupos musicales preferidos, información que la empresa vendió posteriormente a agentes intermediarios de datos en al menos treinta mil ocasiones, sin obtener el previo consentimiento paterno como exige la ley[27]. Pero ¿qué lleva a empresas venerables como McDonald's, Google, Facebook, General Mills y Sony a cometer este tipo de actos? En pocas palabras: hay grandes sumas de dinero en juego y merece la pena correr el riesgo, pues las recompensas son exorbitantes.

Las cosas más caras en la vida son gratuitas

El principio empresarial que la mayoría de internautas no entienden es que están pagando por los llamados servicios gratuitos que reciben en línea, y pagándolos con creces. Ese ruido de succión que escuchas es tu privacidad, tus datos y todos los detalles que componen tu identidad única al ser engullidos por ese gigantesco aspirador que es Internet. Los detalles de tus búsquedas, cosas que no osarías compartir ni con tus mejores amigos o familiares más allegados, se filtran en un gran algoritmo informático en el cielo, se agregan a petabytes y se venden por miles de millones. Eso explica que puedas efectuar búsquedas gratuitas y, pese a ello, el valor de Google ascienda a 400 000 millones de dólares[28]. Todo eso es gracias a ti: su mercancía. Es el trato que has hecho, tanto si eres consciente de ello como si no.

Los ingresos consolidados de Google en 2013 superaron los 59 000 millones de dólares. Esa cantidad representa la diferencia entre cuánto vale tu privacidad para los anunciantes de Google y cuánto te están dejando de pagar. Google obtiene 59 000 millones de dólares y tú obtienes una cuenta de correo electrónico y un buscador web gratuito. Un estudio publicado por el *Wall Street Journal* antes de la oferta pública inicial de Facebook calculaba el valor de cada usuario de Facebook a largo plazo en 80,95 dólares para la empresa[29]. Cada uno de tus amigos valía 62 centavos y tu página de perfil, 1800 dólares. Una página web empresarial y los ingresos por publicidad asociados valían aproximadamente 3,1 millones de dólares para la red

social.

Visto de otro modo, los más de mil millones de usuarios de Facebook, cada uno de los cuales actualiza su estado, detalla su biografía y publica fotografía tras fotografía, se han convertido en la mano de obra gratuita más extensa que ha existido nunca en la historia. Como resultado de su trabajo gratuito, Facebook tiene un valor en mercado de 182 000 millones de dólares y su fundador, Mark Zuckerberg, tiene un patrimonio neto personal de 33 000 millones de dólares. ¿Qué has obtenido tú con el trato? Tal como el científico informático Jaron Lanier nos recuerda, una empresa como Instagram, adquirida por Facebook en 2012, no valía mil millones de dólares porque sus trece empleados fueran «extraordinarios, sino que su valor estriba en los millones de usuarios que realizan aportaciones a la red sin cobrar»[30]. Su inventario son los datos personales, los tuyos y los míos, que vende una y otra vez a terceras partes desconocidas en todo el mundo[31]. En resumidas cuentas, eres una cita barata. Has indicado alegremente a las empresas de Internet todo lo que sabes, todo lo que haces y todos los lugares que visitas a cambio de un pequeño producto o una pizca de entretenimiento.

Y por si ese trato de dinero efectivo a cambio de datos no fuera ya lo bastante cruel, Google ha decidido aumentar su valoración en 400 000 millones de dólares utilizándote a ti y tus fotos en sus anuncios. En octubre de 2013, la empresa anunció una nueva función, conocida como «recomendaciones compartidas», que comenzaron a aparecer en las búsquedas, mapas y los resultados de la tienda Google *Play*. De manera que si, por ejemplo, habías puntuado una canción con cinco estrellas en la tienda de música Google *Play* o habías validado con un pulgar hacia arriba el bar o la panadería del barrio, Google se otorgaba el derecho a vender tus gustos, nombre y promoción a empresas publicitarias y agentes intermediarios de datos. Así, cuando tus amigos Charlie y Juanita busquen una canción o un bar en Google, verán tu rostro sonriente recomendando el producto junto a sus resultados de búsqueda[32]. A George Clooney y Angelina Jolie les pagan por hacer publicidad; ¿y a ti?

Google introdujo las «Recomendaciones compartidas» después de que Facebook estableciera un programa similar muy polémico llamado «Historias patrocinadas» como parte del cual la empresa utilizaba tus «Me gusta» para promocionar a sus verdaderos clientes: los anunciantes y los productos que representaban[33]. Tras la presentación de una demanda colectiva contra Facebook, la red social puso fin a la polémica función, no sin antes haberse embolsado 230 millones de dólares durante los dieciocho meses en los que el programas permaneció activo. Al final, Facebook llegó a un acuerdo con los demandantes por unos 20 millones de dólares, lo cual equivale a unos dos centavos por cada usuario. Es posible que a estas alturas te preguntes: «Pero ¿cómo se pueden salir con la suya?». La respuesta es muy sencilla: se lo has permitido tú.

Términos y condiciones (en tu contra)

> «He leído y acepto los términos y condiciones de este servicio» es la mayor mentira de la Red.
>
> *Terms of service: didn't read*, http://tosdr.Org

Todos los hemos visto. Esos descargos de responsabilidad de cincuenta páginas de longitud escritos en un tipo de letra de cuatro puntos, con interlineado sencillo y márgenes de cinco milímetros. Están diseñador para que resulten imposibles de leer… así que no los leemos. No los leemos y no los entendemos, y pagamos un precio muy alto por ello. En el mundo actual, todos los sitios de Internet, contratos de teléfono móvil, suscripciones a televisión por cable y tarjetas de crédito tienen sus propios términos y condiciones de servicio. Dichos términos delinean cómo pueden succionarse tus datos personales para emplearse de modos inimaginables, incluidos muchos a los que nos opondríamos… si fuésemos capaces de entender el contrato que estamos firmando.

Según un estudio de la Carnegie Mellon University, el estadounidense medio topa con 1462 políticas de privacidad al año, cada una de ellas con una longitud media de 2518 palabras. Si tuviéramos que leer todas esas políticas, tardaríamos setenta y seis jornadas laborales de ocho horas diarias íntegras en hacerlo[34]. En total, eso supone 53 800 millones de horas para el conjunto de los estadounidenses, lo cual representa unos costos de sustitución aproximados a nivel nacional de 781 000 millones de dólares anuales perdidos en productividad debido a la pesadilla y la desgracia que constituyen los términos y condiciones de servicio.

Por supuesto, si todo se redujera a un asunto de productividad perdida, podría no parecer tan insultante, pero estas políticas afectan directamente a nuestros bolsillos. Un estudio realizado por el *Wall Street Journal* calculaba que el lenguaje unilateral de los términos y condiciones de servicio cuesta a cada hogar estadounidense 2000 dólares anuales (un total de 250 000 millones de dólares), un dinero que nos estafan por el hecho de tener toda la baraja de cartas en nuestra contra[35]. Pese a que las empresas denominan a estas políticas «términos y condiciones de servicio», por lo que concierne a los consumidores sería más adecuado utilizar la expresión «términos y condiciones de abuso».

Veamos, por ejemplo, cuánto te cuesta utilizar un sitio de redes sociales, en este caso LinkedIn, cuya política de privacidad establece:

> Otorgas a LinkedIn la siguiente licencia no exclusiva: el derecho irrevocable, mundial, perpetuo, ilimitado, transferible, sujeto a sublicencia, completamente pagado y libre de derechos de autor para copiar, preparar obras derivadas, mejorar, distribuir, publicar, eliminar, retener, añadir, procesar, analizar, utilizar y comercializar de cualquier modo conocido o que se descubra en el futuro, toda la información que proporciones a LinkedIn, de manera directa o indirecta, inclusive, aunque no de manera exclusiva, cualquier contenido generado por el usuario, ideas, conceptos, técnicas y/o datos para

> los servicios que aportes a LinkedIn, sin ningún consentimiento adicional, notificación y/o compensación para ti o un tercero. Cualquier información que nos proporciones puede perderse a tu propio riesgo y cuenta.

De modo que, por usar LinkedIn, otorgas a la empresa un acceso irrevocable y perpetuo (gratuito) a cualquier información que hayas publicado alguna vez en su sitio web; no hay vuelta atrás, no se contempla el empezar de cero. Una vez LinkedIn conoce tus datos, gráfico de red social, historia laboral, capacidades y educación, puede venderlos ahora o en el futuro, como desee, inclusive mediante medios que aún no se han descubierto (por ejemplo, ¿podrían ser poseedores de los derechos holográficos perpetuos de tus imágenes para utilizarlas en publicidad?). Para demostrar lo ridículas que se han vuelto las políticas de privacidad últimamente, el minorista británico GameStation llevó a cabo un experimento con el fin comprobar si alguien se leía alguna vez sus términos y condiciones de servicio. La empresa corrigió su política de privacidad, de manera que dijera:

> Al realizar un pedido a través del sitio web de GameStation el primer día del cuarto mes del año 2010 Anno Domini, nos otorgas una opción intransferible de reclamar, ahora y para siempre más, tu alma inmortal. Si decidiéramos ejercer esta opción, acuerdas entregar tu alma inmortal, y cualquier reclamación que tengas sobre ella, en los 5 (cinco) días laborables siguientes a recibir la notificación por escrito de gamesation.co.uk o uno de sus secuaces debidamente autorizados.

Así es: los 7500 clientes de GameStation que compraron algo en el sitio web el día en el que realizó este experimento otorgaron de manera irrevocable sus almas inmortales al minorista online británico. Sin embargo, por irreverente que fuera su modo de demostrar el hecho de que nadie se lee los términos de servicio, lo cierto es que no son algo que deba tomarse a risa y tribunales de todo el mundo han determinado que, cuando los aceptas con un clic del ratón, te estás vinculando legalmente, con importantes implicaciones económicas, de seguridad y privacidad para ti[36].

Prácticamente todas las empresas de Internet tienen políticas igual de draconianas en tu contra. Si bien la mayoría se frenan y no reclaman tu alma inmortal, muchas están bastante cerca de hacerlo y cuantas más palabras utilizan, peor para ti. La política de privacidad de Facebook ha aumentado de 1004 palabras en 2005 a 9300 en 2014 (sin contar los enlaces a subpolíticas, términos y condiciones varios[37]). Para ponerlo en perspectiva, la política de privacidad de Facebook duplica en longitud la Constitución de Estados Unidos. Por su parte, la política de privacidad de PayPal y sus enmiendas son las más extensas del sector, con 36 275 palabras. Baste decir que *Hamlet* de Shakespeare en inglés tiene 30 066 palabras, incluido en ellas el soliloquio del «Ser o no ser» y el conmovedor discurso final del «Buenas noches, dulce príncipe»[38]. Para complicar aún más las cosas, Facebook y otros se otorgan pleno derecho de modificar sus políticas de privacidad a su voluntad, y lo hacen con cierta

frecuencia.

Peor aún, muchas empresas hacen que acceder a su configuración de privacidad y comprenderla resulte casi imposible[39]. Facebook tiene cincuenta ajustes de privacidad distintos con 170 opciones, mucho más allá del entendimiento del ser humano medio, y eso es precisamente lo que se pretende. Es más, incluso si invertiste en su día las horas que fueran precisas en personalizar las opciones de privacidad, cualquier actualización que Facebook haga a sus términos y condiciones de servicio devuelve automáticamente a todos sus usuarios a los ajustes por omisión, que garantizan el máximo nivel de apertura (para poder vender más su producto, tú, a sus verdaderos clientes, los anunciantes[40]). A menos que compruebes con frecuencia esos ajustes, cosa que deberías hacer, descubrirás que Facebook ha desatendido completamente los ajustes de privacidad explícitos que habías establecido previamente. Como resultado, Facebook se reserva la capacidad de monetizarte sin que su cadena de montaje de humanos ruidosos provoque ninguna interferencia o cacofonía.

Tres meses después de ser adquirida por Facebook, Instagram indignó a sus usuarios al anunciar que vendería sus nombres, imágenes y fotografías a sus anunciantes[41]. De acuerdo con sus términos de servicio actualizados, Instagram argumentó que los padres que habían publicado fotografías de sus hijos menores de edad habían consentido implícitamente el uso de esas imágenes con fines publicitarios. La fotografía de tu hijo que habías subido para compartirla con tus padres podía utilizarse así para vender comida para bebés porque Instagram se había autootorgado tales derechos. ¿Y qué hay de tu magnífica fotografía de la puesta de sol sobre Manhattan? Pues podía venderse como imagen de archivo a diarios y revistas. Como resultado de su cambio en los términos y condiciones de servicio, Instagram se hacía ahora con los derechos intelectuales de los dieciséis mil millones de fotografías de los usuarios, lo cual explicaba por qué Facebook había pagado mil millones de dólares por una empresa con sólo trece empleados.

Google también ha demostrado su inclinación por unos términos de servicio ridículos. Por ejemplo, cualquiera que utilice Google Docs o cargue una hoja de cálculo, PDF o documento de Word en Google Drive otorga automáticamente la propiedad del documento a Google. De acuerdo con los términos de servicio de Google.

> Al subir, almacenar o recibir contenido o al enviarlo a nuestros Servicios o a través de ellos, concedes a Google (y a sus colaboradores) una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas (por ejemplo, las que resulten de la traducción, la adaptación u otros cambios que realicemos para que tu contenido se adapte mejor a nuestros Servicios), comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido[42].

Párate a pensarlo un momento. Si J. K. Rowling hubiera escrito *Harry Potter* en Google Docs en lugar de en Microsoft Word, habría otorgado a Google los derechos

mundiales de su obra, el derecho a adaptarla o de dramatizar los muggles según Google considerara oportuno, por no hablar ya del Colegio Hogwarts de Magia y Brujería. Google habría retenido los derechos de vender sus novelas a estudios de Hollywood y a salas de teatros de todo el mundo, además de disponer de los derechos de traducción. Si Rowling hubiera escrito su épica novela en Google Docs, habría otorgado a Google los derechos de su imperio Harry Potter, valorado en 1500 millones de dólares, y todo porque así lo estipulan los «Término de uso».

El hecho de que Facebook, Google, Twitter y otras empresas guarden tus datos online y obtengan por ellos los máximos beneficios posibles no debería sorprenderte. En cambio, lo que sí puede sorprenderte es el número creciente de plataformas a través de las cuales los anunciantes pueden recopilar y procesar información sobre ti, incluido el teléfono, que en el pasado era inocuo. Alexander Graham Bell quedaría atónito al ver cómo su invento se ha transformado en los teléfonos inteligentes y las aplicaciones de hoy en día, cada una de las cuales ahonda cada vez más en nuestras vidas, con riesgos notables para nuestra privacidad y libertades.

Yo móvil

> Vale, mi teléfono. Cuando aparecieron estas cosas, eran súper *guays*. Nos dimos cuenta demasiado tarde de que, de hecho, eran tan *guays* como los chips electrónicos que ponen a los reos de las prisiones preventivas.
>
> DAVID MITCHELL, *Escritos fantasma*

En la actualidad hay más teléfonos móviles que personas en el planeta, por lo que una red digital omnipresente ha empezado a envolver la Tierra, con consecuencias para todos[43]. Los *smartphones* actuales son potentes ordenadores en miniatura que llevamos encima las 24 horas, los siete días de la semana, y se han convertido en una parte indispensable de nuestras vidas. El 73 por ciento de los norteamericanos admiten que comprueban sus teléfonos cada hora y en torno al diez por ciento lo hace cada cinco minutos[44]. Nos llevamos estos dispositivos al lavabo, al gimnasio y a la cama. Los teléfonos móviles y las tabletas han sustituido a nuestras cámaras, ordenadores, calculadores, calendarios, agendas, radios, televisiones y juegos. De hecho, los usuarios de *smartphones* utilizan sus móviles para navegar por la red, participar en las redes sociales, jugar a juegos y escuchar música, y sólo en quinto lugar para efectuar llamadas[45]. Estos dispositivos forman parte integral de nuestras vidas, y el 84 por ciento de nosotros admite que no podría pasar ni un día sin el móvil[46]. Los teléfonos inteligentes son nuestros escuderos y, como tales, tienen acceso ilimitado a nuestras vidas cotidianas. Ahora bien, ¿les hemos granjeado tal acceso sin meditar bien qué significa compartir la vida virtual con un ordenador que

llevamos encima las veinticuatro horas del día?

Porque, por muy ubicuos y útiles que sean los teléfonos móviles, también son verdaderos soplones en nuestros bolsillos, espías digitales que rastrean cada uno de nuestros movimientos. Ese dispositivo que llevas en el bolso o en los tejanos pensando que es sólo un teléfono móvil, en realidad es un faro que envía señales al mundo constantemente y proporciona un flujo de datos incesante acerca de ti, de tu ubicación y de tus actividades vitales[47]. Sólo en Estados Unidos, los teléfonos móviles generan en torno a 600 000 millones de eventos de datos únicos cada día, inclusive dónde estás, a quién has enviado mensajes de texto y qué fotografías has publicado en Internet[48]. El volumen de datos que filtramos a través de nuestros ordenadores en casa y en el trabajo se queda en mantillas en comparación con lo que filtramos a través de esos compañeros digitales que llevamos en el bolsillo. Los teléfonos móviles proporcionan la imagen más nítida de los hábitos y las preferencias de una persona, o lo que es lo mismo: de su vida[49]. Pero ¿quién tiene acceso a estos datos? Muchas más personas de las que crees. Saber dónde te encuentras, dónde pasas el tiempo, en qué inviertes el dinero y con quién brinda más posibilidades de minar tu información, que cada vez es más valiosa. Los agentes intermediarios de datos, espías y delincuentes por igual han acabado por entender que el teléfono móvil es una importantísima fuente de espionaje para sus objetivos. En consecuencia, ellos, como muchos otros, contemplan los móviles inteligentes como artilugios para saciar su sed de venganza.

La oportunidad de poseer todos tus datos móviles fue el motivo que impulsó a Google a crear su sistema operativo para teléfonos móviles Android y entregarlo de manera gratuita tanto a los desarrolladores como a los usuarios. Sin embargo, tal como hemos visto con anterioridad, lo gratuito puede salirnos muy caro. El *software* de los teléfonos móviles Android proporciona a Google tu número de teléfono, información de red, datos de almacenamiento en el dispositivo, registros de llamadas y listas de contactos, además de una serie de sensores capaces de detectar tus movimientos, ubicación e incluso la temperatura ambiental, la humedad y el volumen de ruido local[50].

Una vez lanzados todos estos anzuelos tecnológicos a tu vida, Google no perdió el tiempo en rellenar una solicitud de patente bajo el epígrafe «Publicidad basada en condiciones ambientales»[51]. ¡*Piticlín piticlín*! Ahora Google puede detectar si estás en una ubicación donde hace calor y, en función de ello, presentarte un anuncio de aire acondicionado o de helado. Gracias a su tecnología para detectar el sonido ambiental, Google también puede escuchar el sonido de fondo que se oye mientras llamas por teléfono para ofrecerte anuncios basados en tales preferencias[52]. De manera que, si por casualidad escuchas a Usher de fondo mientras hablas con tu tía Margarita desde tu teléfono Android, Google tiene la capacidad de detectarlo y te mostrará anuncios de sus próximos conciertos la próxima vez que compruebes tu cuenta de Gmail o efectúes una búsqueda en la Red.

También Facebook ha incorporado ahora la capacidad de utilizar el micrófono de tu teléfono para escucharte y escuchar los sonidos cercanos, todo ello conforme a sus términos de uso actualizados y como parte de su gran apuesta por los usuarios de móviles[53]. Cuando, en el cuarto trimestre de 2013, Facebook reveló que había alcanzado la cifra de 945 millones de usuarios móviles mensuales y que el 53 por ciento de sus ingresos procedían de la publicidad en los móviles, el mercado mostró su adoración por la empresa y añadió miles de millones de dólares a su cotización en los días posteriores a tal anuncio[54]. Al crear finalmente su aplicación móvil, Facebook no sólo diseñó una mejor experiencia para el usuario, sino también una nueva herramienta para obtener cantidades ingentes de datos de los dispositivos móviles de éste.

¿Quién te roba los datos? También hay una aplicación para eso

Un anuncio del iPhone de Apple de 2009 nos presentó a todos el célebre eslogan «Hay una aplicación para eso», con el que nos indicaba que existe una aplicación de iPhone para cualquier necesidad humana concebible. En su momento era una declaración osada, pero quizá Steve Jobs estuviera en lo cierto. Desde su lanzamiento en 2008, se han registrado más de sesenta y cinco mil millones de descargas de la tienda App Store de Apple, las cuales generaron más de 10 000 millones de dólares en ingresos sólo en 2013[55]. Para competir con Apple, Google lanzó su propia tienda de aplicaciones, llamada Google *Play*, y cada empresa alberga más de un millón de aplicaciones propias disponibles para su descarga. El ritmo al cual se multiplican estos pequeños programas informáticos llamados aplicaciones o *apps* es sensacional, pero ¿qué motiva a decenas de miles de programadores de todo el mundo a crear aplicaciones? El dinero, por supuesto. Sí, pero ¿cómo ganan dinero si la mayoría de las aplicaciones son gratuitas? Pues, como hemos visto antes, lo gratuito es un magnífico modelo de negocio, siempre y cuando capitalices a las personas apoderándote de sus datos personales, en volúmenes gigantescos. Y resulta que las aplicaciones son un magnífico ecosistema para hacer exactamente eso. Ello ayuda a explicar también por qué empresas como Rovio (creadora del archiconocido juego *Angry Birds*) han pasado de estar prácticamente en la oscuridad a contar con una valoración de mercado de nueve mil millones de dólares en cuestión de pocos años[56].

Tal como los cigarrillos no son más que sistemas de provisión de nicotina eficaces, las aplicaciones no son más que herramientas elegantes y sumamente eficaces para trasmitir tus datos privados a los anunciantes (con la diferencia de que

los cigarrillos, por lo menos, están regulados). La cantidad de información personal que te hurta el teléfono móvil mediante las aplicaciones es impactante. Por ejemplo, el mero acto de descargarte la aplicación de Facebook en un móvil Android comparte automáticamente el número de teléfono con la red social, incluso antes de que el usuario se haya registrado en ella o haya manifestado su acuerdo con los términos de servicio[57]. Una vez descargado Facebook, los usuarios aceptan sus términos de servicio y le conceden el derecho a «tomar fotografías y vídeos con la cámara», un ajuste que permite a Facebook activar la cámara de tu teléfono móvil en cualquier momento sin previa confirmación por tu parte[58]. Los términos y condiciones de servicio de la red social también la autorizan a leer tus mensajes de texto. En el pasado reciente, Facebook empezó a solicitar a centenares de millones de usuarios de su aplicación móvil que activaran la nueva opción de «Sincronización de fotos» para cargar automáticamente cada imagen tomada con el teléfono a los inmensos servidores de datos de la red social[59].

Pese a que Facebook sostiene que, en realidad, no activa tu cámara ni lee tus mensajes, se ha reservado el derecho de hacerlo. Pero, francamente, ¿cómo puede saber el usuario qué datos le están sacando del teléfono? Todo esto tiene lugar en segundo plano, de manera oculta en el trasfondo de la aplicación, y no se contempla mostrarlo a aquellas personas que Facebook ha convertido en su producto.

La apropiación de tu información personal identificativa (IPI) acontece en el momento en el que aceptas descargar una aplicación. Así por ejemplo, cuando adquieres una aplicación para Android en la tienda Google *Play*, Google proporciona a la empresa de la aplicación tu nombre completo, tu dirección de correo electrónico y tu dirección postal. Esto tiene lugar sin una advertencia clara cada vez que te descargas una aplicación[60]. Pero ¿quiénes son exactamente estas empresas de aplicaciones (miles de ellas repartidas por todo el mundo) que conocen tu nombre, dirección y número de teléfono? ¿Qué políticas de privacidad implementan y qué hacen con esta información? ¿Con qué grado de seguridad la almacenan y a quién se la venden? La verdad es que Internet es una jungla y apenas existen leyes que te protejan o protejan de manera eficaz tus datos de estos vendedores ambulantes de información externos. Al compartir millones de nombres y datos de contacto con sus vendedores de aplicaciones, Google aumenta la probabilidad de que tus datos se filtren, sean robados o se utilicen de manera indebida.

Como sospecharás llegados a este punto, los populares juegos para Facebook creados por Zynga —*FarmVille, Texas Hold'Em Poker* y *Mafia Wars*— son gratuitos porque también ellos sustraen tu IPI, incluidos los nombres de todos tus amigos de Facebook[61]. Esta información se vende a docenas de empresas de publicidad y rastreo por Internet, incluso aunque tengas los máximos ajustes de privacidad configurados. Y aunque colocar pájaros en tirachinas y lanzárselos a cerdos que roban huevos puede ser divertido, tal como atestiguan los mil millones de usuarios que se han descargado la aplicación *Angry Birds*, el juego tiene una capacidad voraz

de recopilar información personal de sus usuarios, incluidas las localizaciones a las que viajan con sus teléfonos móviles[62]. Pese a ello, un estudio realizado por el Human-Computer Interaction Institute de Carnegie Mellon reveló que sólo el cinco por ciento de los usuarios de *Angry Birds* sabían que la empresa almacenaba los datos de su ubicación para rastrearlos en el mundo real con fines publicitarios y comerciales. Ahora bien, *Angry Birds* dista mucho de ser el único infractor. McAfee informó de que el 82 por ciento de las aplicaciones para Android realiza un seguimiento de tus actividades en Internet y un 80 por ciento recaba información acerca de tu ubicación[63].

Ubicación: la importancia del lugar

Para los anunciantes, hay tres preguntas clave: ¿quién comprará sus productos?, ¿qué buscan los clientes? y ¿dónde están? En el mundo en línea, Google ganó por goleada la pregunta «qué» hace mucho tiempo con sus potentes algoritmos de búsqueda. Google sabe lo que buscas e incluso rellena la casilla de búsqueda de la parte superior de la pantalla antes de que hayas acabado de teclear tu pregunta. Facebook sabe «quién», pues te conoce a ti y conoce tu red social en mayor profundidad que ninguna otra empresa. Pero el «dónde» aún no es propiedad en exclusiva de ninguna empresa y se está librando una batalla entre los titanes existentes y una raza de nuevas *start-ups* que pretenden hacerse con este factor a toda costa. Presentarte un anuncio o un cupón de yogur helado cuando te acercas a una heladería es lo más parecido al nirvana de la publicidad. Hasta ahora, la tecnología para hacer algo así no existía, pero todo eso cambió con la revolución de los teléfonos móviles, lo cual explica que se haya desatado la fiebre del oro por conocer los datos de tu ubicación. McKinsey ha calculado que el valor de mercado de los datos sobre tu ubicación personal ha superado los cien mil millones de dólares para las empresas al por menor, de telecomunicaciones y contenido en los últimos diez años[64].

El «dónde» se determina mediante diversas técnicas: la antena de GPS de tu teléfono, triangulando la ubicación de tu móvil y la distancia entre las antenas de telefonía móvil e incluso mediante las redes Wi-Fi a las que te conectas. Los datos de tu ubicación se anexan a un número creciente de tus transacciones en línea, en los llamados metadatos de archivo, a saber: los datos que proporcionan datos acerca de información adicional. Por ejemplo, cuando la mayoría de las personas toman una fotografía con sus teléfonos móviles, los datos de la ubicación (coordenadas de GPS, longitud, latitud, etc.) se incrustan al archivo de la imagen. Y cuando esas fotografías y vídeos se publican en Craigslist, Flickr, YouTube, Facebook y cientos de servicios adicionales, estos metadatos reveladores se envían junto con el archivo original. En

algunas aplicaciones, como en Google Maps o las herramientas de navegación mediante GPS, que se solicite la ubicación es perfectamente lógico. En cambio, en otras, registrar tu localización proporciona a los creadores de aplicaciones otro modo de vender tus datos a un mayor precio.

Tus publicaciones en Facebook, tus tuits y tus búsquedas en Yelp incluyen tus datos de localización. Es más, cada vez son más las empresas noveles de servicios basados en la localización (SBL) que están incorporando tu «dónde» a todo, desde tus compras cotidianas hasta tus propiedades inmobiliarias. Quizá uno de los nichos con un crecimiento más acelerado en las aplicaciones SBL sean las que tienen que ver con las relaciones personales y el amor, sobre todo el «amor» de duración limitada. Aplicaciones como Tinder y Grindr se han descargado millones de veces y pueden ser responsables de más de cincuenta millones de relaciones esporádicas, de acuerdo con el director ejecutivo de Tinder[65]. Ah, las aplicaciones del amor… esa cosa tan esplendorosa.

Pero todos los beneficios potenciales de estos nuevos flujos de datos de localización conllevan también nuevos riesgos. En 2012, una empresa rusa lanzó una aplicación llamada Girls Around Me, que recibió la aprobación para figurar tanto en la tienda de Apple App Store como de Google *Play*[66]. Girls Around Me aprovechaba todas las publicaciones, actualizaciones de estatus, fotografías y accesos a lugares públicos que incorporaban metadatos de ubicación posteados por mujeres en servicios como Facebook y Foursquare. Cuando un usuario abría la aplicación Girls Around Me en su teléfono, sólo necesitaba pulsar un botón para que le apareciera un mapa interactivo con los rostros de las mujeres jóvenes que había a sus alrededores y sus ubicaciones exactas. Con el «modo de radar» de la aplicación, cualquiera podía geolocalizar a estas mujeres y ver sus perfiles de Facebook.

Por ejemplo, si un hombre utilizaba Girls Around Me y veía que una joven atractiva acababa de entrar en la cafetería Starbucks del barrio, podía realizar su seguimiento, acceder a su perfil de Facebook y comprobar a qué escuela o universidad había asistido, si recientemente había estado de vacaciones en Las Vegas o los nombres de sus padres, su bebida favorita y si ese mismo día había visto un capítulo de *Orange Is the New Black* en Netflix. Armado con esta información, el hombre, un completo extraño, podía acercarse de manera informal a la joven mientras hacía cola para pedir su café con leche de soja extracaliente grande diario y entablar una conversación sobre cuánto le gustaban Las Vegas y *Orange Is the New Black*. Una herramienta potentísima para flirtear, y también para los acosadores y violadores en busca de mujeres de su interés.

Para los anunciantes, no obstante, ese «dónde» no se corresponde exclusivamente a tu localización actual, sino que también les interesa dónde estuviste ayer y el mes pasado, y dónde es probable que estés mañana. Los registros de localización detallan exactamente cuánto tiempo pasaste en Zara frente a Mango, y la secuencia de estos movimientos es mucho más reveladora. En el mundo en que vivimos, donde la

publicidad se canaliza en función de la ubicación de los posibles clientes, cuando una mujer se lleva el teléfono móvil (con sus aplicaciones incluidas) a la consulta del ginecólogo, se registra un punto de referencia interesante en todo el ecosistema de la publicidad móvil. Y cuando esa misma mujer tres semanas más tarde entra en una tienda de ropita o juguetes para bebés, se revela potencialmente una verdad mucho más profunda. Al ir sumando los datos de tu localización a lo largo del tiempo, los anunciantes pueden deducir si vas a la iglesia o a la sinagoga, si haces deporte en un gimnasio, si acostumbras a tomar una copa en un bar del barrio, si visitas a un psicólogo o si estás engañando a tu pareja[67]. Pero ¿quién es exactamente esta gente que está recopilando toda esta información? ¿Cuánta información tienen? ¿Y qué hacen con ella? Como estás a punto de descubrir, manejan volúmenes inmensos de datos, que se multiplican exponencialmente para usos varios y cuyo contenido ni siquiera han empezado a identificar todavía[68].

Capítulo 5

La economía de la vigilancia

> En la era digital, la privacidad debe ser una prioridad. ¿Me lo parece a mí o la vigilancia generalizada en secreto es una atrocidad y una obscenidad?
>
> AL GORE

Leigh Van Bryan estaba contentísimo porque iba a viajar a Estados Unidos por primera vez de vacaciones[1]. Unos días antes de su viaje a Los Ángeles, el joven británico de veintiséis años contactó con una amiga por Twitter y le preguntó si «estaba libre esta semana para cotillear un poco antes de que me vaya a destruir América». Cualquier joven veinteañero del Reino Unido habría entendido que el uso de la palabra «destruir» por parte de Van Bryan era metafórico, una manera de decir «salir de fiesta y pasármelo en grande» en lenguaje de la calle. Por desgracia, lo que menos hizo Van Bryan al llegar a Estados Unidos fue divertirse.

El Departamento de Seguridad Nacional estadounidense había estado monitorizando ampliamente las redes sociales en busca de posibles amenazas contra el país y Van Bryan había quedado atrapado en su web. A su llegada a Los Ángeles, Van Bryan y su compañera de viaje, Emily Bunting, de veinticuatro años, fueron recibidos por agentes de Aduanas y Protección de Fronteras armados y pasaron en el calabozo doce horas, junto con supuestos narcotraficantes mexicanos. Pese a que la pareja intentó explicar el uso en argot de la palabra «destruir», los funcionarios estadounidenses se negaron a prestarles atención. Los agentes federales buscaron y rebuscaron en las maletas de ambos y los sometieron a cacheos reiterados. Inexplicablemente, buscaban palas. Resultó ser que otro tuit acerca de «cavar la tumba de Marilyn Monroe» —un guiño a un episodio de los dibujos animados *Padre de familia*— también había levantado las banderas de alarma en el Departamento de Seguridad Nacional, que temía por los restos de la desaparecida actriz. Tras una noche incómoda en celdas separadas, Van Bryan y Bunting se reunieron, justo a tiempo para ser devueltos en un avión de regreso a Reino Unido. Les habían denegado la entrada en Estados Unidos y fueron deportados a Gran Bretaña. Al final, lo único que se destruyó fueron sus visados y sus vacaciones.

¿Pensabas que los *hackers* eran los malos de la película? Espera a conocer a los agentes intermediarios de datos

Acxiom, Epsilon, Datalogix, RapLeaf, Reed Elsevier, BlueKai, Spokeo y Flurry: la mayoría de nosotros nunca hemos oído hablar de estas empresas, pero junto con algunas otras son las responsables del sector emergente de la vigilancia de datos, el cual mueve 156 000 millones de dólares al año. Y aunque ciudadanos de alrededor del mundo quedaron conmocionados al tener noticia del tamaño y el alcance de las operaciones de vigilancia que llevaba a cabo la NSA reveladas por Edward Snowden, es importante destacar que los 156 000 millones de dólares en ingresos anuales que gana el sector de los intermediarios de datos duplica el presupuesto que el gobierno estadounidense destina a sus servicios de inteligencia[2]. La infraestructura, herramientas y técnicas que emplean estas empresas corresponden casi por entero al sector privado y, sin embargo, el grado en que pueden asomarse a la vida de cualquier ciudadano haría que cualquier agencia de espionaje del mundo se pusiera verde de envidia.

Los agentes intermediarios de datos obtienen su información de nuestros proveedores de servicios de Internet, emisores de tarjetas de crédito, empresas de telefonía móvil, bancos, financieras, farmacias, departamentos de vehículos a motor, supermercados y, cada vez más, de nuestras actividades en línea. Todos los datos que regalamos en nuestro día a día en las redes sociales, cada «Me gusta», toque o tuit, se etiquetan, geocodifican y clasifican para su reventa a los anunciantes y comerciantes. Incluso los vendedores a la antigua usanza empiezan a darse cuenta de que tienen una fuente de ingresos secundaria colosal (los datos de sus clientes) que puede ser incluso más valiosa que el producto o servicio que venden. Así, las empresas se apresuran a sacar partido de este novísimo flujo de ingresos y transforman su infraestructura de datos de un centro de costes en un centro de beneficios. Pese a que financieras como Experian, TransUnion y Equifax hace años que operan en el mundo, nuestro estilo de vida cada vez más conectado digitalmente permite a nuevas empresas recopilar cada pequeño dato de nuestras vidas, en una medida que hasta ahora nos parecía no sólo imposible, sino inconcebible.

Una sola de estas empresas, Acxiom Corporation, ubicada en Little Rock, Arkansas, opera más de veintitrés mil servidores informáticos dedicados a «recopilar, ordenar y analizar» más de 50 000 billones de transacciones de datos únicos cada año[3]. El 96 por ciento de los hogares estadounidenses figuran en estos bancos de datos, y Acxiom ha acumulado más de 700 millones de perfiles de consumidores en todo el mundo. Cada uno de estos perfiles contiene mil quinientos rasgos específicos por persona, incluidos entre ellos la raza, el sexo, el número de teléfono, el tipo de coche que conduce, el nivel de estudios, el número de hijos, los metros cuadrados de su hogar, el tamaño de su currículum, las compras recientes, su edad, su altura, su peso, el estado civil, las opiniones políticas, los problemas de salud, la profesión, si es zurda o diestra y la raza de mascota que tiene, si es que la tiene[4].

El objetivo de Acxiom y de otros agentes intermediarios de datos es proporcionar lo que se conoce con los nombres alternativos de «publicidad comportamental»,

«publicidad predictiva» o «información privilegiada sobre comportamientos básicos» acerca de ti y de tu vida. En lenguaje llano, significa entenderte con una precisión extrema para que los agentes intermediarios de datos puedan vender la información que compilan al mayor precio a los anunciantes, comerciantes y otras empresas para su toma de decisiones. Por ejemplo, mostrar un anuncio de pañales a un estudiante universitario de diecinueve años podría representar una pérdida de presupuesto invertido en publicidad, pero mostrar esa misma información a una ama de casa de treinta y dos años embarazada podría derivar en cientos de dólares en ventas. Para maximizar el valor de los datos digitales que recopilan, los agentes intermediarios de datos nos segmentan a perpetuidad en grupos o perfiles cada vez más específicos. Bienvenido al mundo de la vigilancia de datos.

Acxiom vende estos perfiles informáticos a doce de las quince principales empresas emisoras de tarjetas de crédito, siete de las diez principales bancas personales, ocho de las diez principales empresas de telecomunicaciones y nueve de las diez aseguradoras más importantes[5]. Para ordenar los miles de millones que cobra a sus clientes anunciantes cada año, «Acxiom te asigna un código de 13 dígitos y te clasifica en uno de 70 “clústers” o grupos, en función de tu comportamiento y datos demográficos». A título de ejemplo, las personas incluidas en el clúster 38 «probablemente son afroamericanos o hispanos, padres trabajadores de adolescentes y personas de clase media-baja que suelen comprar en comercios baratos»[6]. Y alguien perteneciente al grupo 48 es probable que sea «caucásico, con estudios superiores, que viva en el entorno rural con su familia y le guste cazar, pescar y ver las carreras de NASCAR». Estos datos se venden a otros agentes externos, que aplican sus propios algoritmos y refinan aún más los conjuntos de datos para crear listas de categorías propias, como «familias católicas», «jugadores compulsivos online», «movilidad nula» e «hispanos con anticipos o créditos fáciles»[*].

Los incluidos en la categoría de familias católicas pueden recibir anuncios de Biblias y de la web relacional ChristianMingle.com, mientras que a los jugadores y a aquéllos clasificados por el algoritmo como personas con «movilidad nula» se les presentarán anuncios de prestamistas de dinero fácil y programas de consolidación de deudas[7]. Y pese a que aparecer listado como familia católica o mujer hispana con estudios superiores y urbanita puede, aparentemente, no resultar ningún problema, algunos agentes intermediarios de datos han vendido listas mucho más preocupantes a anunciantes y otros interesados anónimos. Por ejemplo, algunos agentes de datos ofrecen listas de personas de la tercera edad con demencia y de enfermos con sida, mientras que otra empresa, MEDbase200, ha llegado a subastar listas con nombres de víctimas de violencia doméstica y supervivientes de una violación[8].

La profundidad y el alcance de la economía de la recopilación y vigilancia de datos comerciales quedó subrayada a principios de 2014 cuando un habitante de Lindenhurst, Illinois, que había perdido a su hija recibió un folleto publicitario por correo del minorista OfficeMax. En la etiqueta de la dirección aparecían impresas las

palabras siguientes: «Mike Seay, hija muerta en accidente de tráfico», seguidas de la dirección postal del hombre[9]. En efecto, OfficeMax había dado con la persona correcta: la hija de diecisiete años de Seay había muerto en un accidente de tráfico con su novio el año previo. Cuando Seay telefoneó a OfficeMax para quejarse acerca de aquel incidente, el director se negó a creerle y desestimó sus alegaciones tildándolas de «imposibles». OfficeMax no reconoció que el error era «el resultado de una lista de correo alquilada a un proveedor externo» hasta que un periodista de la NBC de Chicago escribió un artículo sobre aquel caso[10]. Finalmente, Seay recibió una llamada telefónica de disculpa de un ejecutivo de nivel inferior de OfficeMax, quien, no obstante, se negó a responder a la solicitud reiterada de Seay de conocer el nombre del agente intermediario de datos responsable de aquel suceso. En la misma línea, el ejecutivo se negó a revelar si la empresa contaba con datos similares relativos a otros clientes potenciales. La historia de Seay es sin duda inquietante, sobre todo porque no era un cliente habitual de OfficeMax, sino que únicamente había adquirido papel para la impresora en la tienda de manera esporádica.

Este incidente pone de relieve algunos interrogantes serios acerca del sector de los intermediarios de datos. Por ejemplo, ¿qué otros datos íntimos baraja OfficeMax acerca de sus clientes? Para que el agente intermediario de datos le haya vendido esa información, ¿qué más pueden revelar sobre ti y tu familia estos bancos de datos masivos? ¿Tal vez que tienes un hermano alcohólico? ¿O que tu madre está diagnosticada de esquizofrenia? ¿Quizá que tu hija de trece años tiene una trastorno alimentario? ¿Qué regulaciones existen que pongan freno a lo que los agentes intermediarios de datos pueden hacer con esa información y qué puedes hacer tú si la información sobre ti que tienen es incorrecta? Pues la verdad es que apenas existen leyes al respecto. Recuerda demasiado al argumento de la célebre novela de Franz Kafka *El proceso*, en la que un hombre es arrestado sin que le informen de los motivos y después descubre que un misterioso tribunal maneja un dosier secreto sobre él, al cual tiene vetado el acceso. Los agentes intermediarios de datos de hoy en día, a diferencia de las agencias financieras, apenas están regulados por el gobierno. No existen leyes, como puede ser la Fair Credit Reporting Act (Ley de información de créditos justos estadounidense), que les exijan proteger la privacidad del cliente, corregir los errores fácticos o incluso revelar qué información almacenan en sus sistemas sobre nosotros y nuestras familias.

A consecuencia de la experiencia de Seay y de otros miles como él, el Congreso estadounidense, liderado por el senador Jay Rockefeller de West Virginia, la Comisión Federal de Comercio y la Oficina de Protección Financiera del Consumidor, han comenzado a investigar la naturaleza y el alcance del multimillonario sector de los agentes intermediarios de datos[11]. Es evidente que dichos agentes se opondrán con vehemencia a cualquier modificación significativa de las leyes, porque hay mucho dinero en juego. Es más, una vez los datos están ahí, es prácticamente imposible volver a meter la pasta dentífrica en el tubo. En el ínterin,

Acxiom y otras empresas continúan cosechando información sobre ti. A finales de 2013, el director ejecutivo de Acxiom, Scott Howe, anunció, orgulloso, que su empresa había recopilado cerca de mil cien millones de *cookies* de terceras partes y había identificado y trazado el perfil de los dispositivos móviles de más de doscientos millones de consumidores. «Nuestro alcance digital en breve llegará a todos los internautas de Estados Unidos», afirmó Howe[12].

Mediante la minería de bases de datos públicas y la adición de ese conocimiento a los datos personales que compartimos, de manera voluntario o involuntaria, acerca de nosotros mismos, de nuestras amistades y familiares en las redes sociales, empresas como Acxiom han logrado desplegar el sistema de vigilancia y espionaje más generalizado que ha existido nunca en las vidas de prácticamente todos los estadounidenses vivos. Este hito tecnológico representa la «nueva normalidad» de la sociedad de la vigilancia de datos en la que vivimos y forma parte de lo que el exvicepresidente de Estados Unidos Al Gore denominó la «economía del acoso» durante una ponencia que impartió en 2013 en el festival interactivo South by Southwest en Austin, Texas.

Al Gore tiene razón. Como debería ser evidente a estas alturas, la vigilancia es el modelo de negocio de Internet. Creamos cuentas «gratuitas» en sitios web como Snapchat, Facebook, Google, LinkedIn, Foursquare y PatientsLikeMe y nos descargamos aplicaciones gratuitas como *Angry Birds*, *Candy Crush Saga*, *Words with Friends* y *Fruit Ninja*, y a cambio, de manera consciente o inconsciente, accedemos a permitir a estas empresas rastrear todos nuestros movimientos, recopilarlos, correlacionarlos y vendérselos al mayor número de personas y al precio más alto posible, sin ninguna responsabilidad ni límite legal, moral o ético. Y pese a ello, somos muy pocos quienes nos detenemos a preguntarnos quién más tiene acceso a estos detritos de datos y cómo puede utilizarlos en nuestra contra. La vigilancia de datos es «el nuevo negro» y sus usos, capacidades y potencia están a punto de brotar como setas de modos que muy pocos consumidores, gobiernos o tecnólogos han osado imaginar.

Cómo te analizan

Cada uno de nosotros deja un rastro digital a lo largo del día, un flujo infinito de registros telefónicos, mensajes de texto, historiales de navegación, datos GPS y correos electrónicos que vivirán toda la eternidad. El análisis de esta información permite a las empresas hallar clientes prospectivos con un grado de precisión muy superior y un valor mucho más elevado de lo que hasta ahora era posible. Pongamos por ejemplo que te gustaría ir con tu familia de vacaciones a Miami Beach. Buscas vuelos en la web de Kayak. Posteriormente entras en una tienda y compras un

bañador con tu tarjeta de crédito. Los datos recopilados a partir de la compra del bañador combinados con tus datos de navegación refuerzan la probabilidad de que te interese reservar una habitación de hotel en Miami. A consecuencia de este análisis del comportamiento, ahora tus datos tienen un valor cuantificable para los hoteles de Miami, que pueden presentar una mejor oferta que la competencia a tiempo real mostrándote publicidad con anuncios relevantes y ofertas basadas en tu comportamiento previsto.

Google Now, que promete «sólo la información oportuna en el momento oportuno», es otro ejemplo de análisis profundo aplicado a grandes conjuntos de datos. La aplicación Google Now proporciona a los consumidores una información maravillosamente práctica que les ayuda a captar y cotejar todos los datos invisibles que se arremolinan a su alrededor. Una vez los usuarios aceptan los términos de servicio de Google, Google Now les muestra cuándo sus amigos están cerca, les proporciona alertas de tráfico, determina los recorridos más rápidos para llegar del hogar al trabajo, muestra automáticamente la predicción del tiempo por la mañana, lleva un seguimiento de tus equipos deportivos favoritos y actualiza los marcadores a tiempo real. Google Now te informa de manera automática de si tu vuelo sale con retraso y si la puerta de embarque ha cambiado, además de ofrecerte vuelos alternativos cuando existen. Dado que Google Now sabe cuáles son todas tus citas y monitoriza los atascos de tráfico en las rutas que tienes previsto utilizar en tiempo real, la aplicación te alertará en tu localización actual y te aconsejará que salgas temprano si quieres llegar a tiempo a tu próxima reunión. Mediante una técnica conocida con el nombre de «geovalla» (*geo-fencing* en inglés), Google Now explora tu lista de tareas pendientes y la coteja con tu ubicación, que rastrea de manera continua con el fin de avisarte de que tienes que comprar leche cuando pasas por delante del supermercado. Para disfrutar de este colmo de la abundancia informativo y de esta práctica munificencia, sólo tienes que proporcionar a Google Now acceso pleno a tu huella digital en línea, incluidos tu buzón de entrada de Gmail, tus búsquedas en la Red, tus reservas de hotel, tus planes de vuelo, tus listas de contacto íntegras, los cumpleaños de tus amigos, tus reservas en restaurantes y tus citas en el calendario, además de tu ubicación en todo momento a través del GPS de tu teléfono móvil. A partir de ese conjunto masivo de datos, Google (y otras empresas) pueden recrear lo que los analistas de inteligencia denominan tu «patrón de vida», lo cual equivale a saber y cartografiar tu localización física a lo largo del tiempo, además de qué haces en cada momento y con quién. Él no va más de la practicidad.

Pero ¿qué más pueden ser capaces de determinar tanto Google como cualquier empresa que tenga acceso a tu patrón de vida? Pongamos, por ejemplo, que tu teléfono móvil pernoctara en la misma vivienda que el teléfono de tu esposa seis noches a la semana. A partir de tales datos, sería lógico inferir que los propietarios de esos dos teléfonos móviles conviven y duermen juntos. Pero ¿qué sucedería si una noche a la semana tu teléfono móvil pernoctara junto al teléfono móvil de otra mujer?

¿Qué podría insinuarle eso a Google u otras empresas acerca de tu fidelidad? El análisis de tus datos de localización y el de los teléfonos (y aplicaciones) que te rodean ofrece una excelente perspectiva de la fortaleza y los lazos de tus redes personales y profesionales. El estudio de tus estelas de datos a lo largo del tiempo puede revelar muchos otros aspectos acerca de tu vida. Por ejemplo, en el Reino Unido, un equipo de investigación estudió las localizaciones pasadas de una serie de usuarios de teléfonos móviles y, aplicando técnicas de análisis de datos básicas, fue capaz de predecir con un margen de error de veinte metros dónde estaría cada usuario de móvil veinticuatro horas después, una herramienta sumamente útil tanto para los anunciantes como para los acosadores[13]. Hoy en día, tu teléfono no sólo sabe dónde has estado, sino también adónde te diriges.

El análisis de tu red social y de sus integrantes también puede ser muy revelador acerca de tu vida, tendencia política e incluso orientación sexual, tal como se demostró en un estudio realizado en el MIT. En un análisis conocido como Gaydar, los investigadores estudiaron los perfiles de Facebook de 1500 alumnos de la universidad, incluidos aquéllos cuya orientación sexual aparecía vacía en el perfil o listados como heterosexuales. A partir de una investigación previa que revelaba que los hombres homosexuales tienen más amigos homosexuales que heterosexuales (cosa que no debería sorprender), los investigadores del MIT contaban con un punto de referencia valioso para revisar los vínculos de amistad de los 1500 estudiantes. Como resultado de ellos, los investigadores estuvieron en disposición de predecir con un 78 por ciento de precisión si un alumno era o no homosexual[14]. Al menos diez personas que previamente no se habían identificado como homosexuales fueron etiquetadas por el algoritmo de los investigadores y confirmaron su inclinación sexual en entrevistas personales[15]. Y mientras que tales averiguaciones pueden no representar ningún problema en Cambridge, Massachusetts, un lugar liberal, sí que podrían resultar problemáticas en países en los que la homosexualidad es ilegal, como Sudán, Irán, Yemen, Nigeria y Arabia Saudí, donde se considera un «delito» penado con la muerte[16]. Un estudio de cincuenta y ocho mil usuarios de Facebook publicado por la Academia Nacional de Ciencias de Estados Unidos demostraba que sólo con estudiar sus «Me gusta» era posible determinar detalles íntimos y rasgos de personalidad con una precisión asombrosa[17]. El riguroso estudio realizado de manera conjunta con la Universidad de Cambridge predecía si los usuarios tenían un cociente intelectual alto o bajo, si eran emocionalmente estables o si procedían de un hogar desestructurado. El desafío que plantean los datos que filtramos es que, tal como se ha demostrado en numerosas ocasiones, otros pueden recoger nuestras migas de pan digitales e interpretarlas sin nuestro conocimiento de modos que pueden ser perjudiciales para nosotros.

No tengo nada que ocultar

En diciembre de 2009, cuando la periodista de la CNBC Maria Bartiromo preguntó al director ejecutivo de Google, Eric Schmidt, acerca de las inquietudes en materia de privacidad que planteaba el creciente rastreo de los consumidores que llevaba a cabo Google, Schmidt dio su famosa respuesta: «Si haces algo que no quieres que nadie sepa, quizá deberías no hacerlo»[18]. Schmidt, entre otros, restaba importancia a las preocupaciones en materia de privacidad alegando que, si no haces nada malo, no tienes por qué temer que nadie, ni empresas, ni gobiernos, ni tus vecinos, sepan en qué inviertes tu tiempo.

Tal argumentación ha encontrado eco en el director ejecutivo de Facebook, el propio Mark Zuckerberg, quien ha argumentado que «la privacidad ya no es la norma por la cual se rige la sociedad»[19]. Y si bien la privacidad puede haber dejado de ser esa norma, al menos para el público general, el señor Zuckerberg parece atesorar bastante su propia intimidad. A finales de 2013 se conoció que el director ejecutivo de Facebook había gastado 30 millones de dólares en comprar las cuatro casas que rodean su vivienda para garantizar que su privacidad no padeciera ninguna intrusión o perturbación.

La directora operativa de Facebook, Sheryl Sandberg, también ha insinuado que la defensa del derecho a la privacidad va en contra de la «verdadera autenticidad». Sandberg observa que «la expresión de la verdadera identidad será cada vez más generalizada en los años venideros […] Y efectivamente, tardaremos en acostumbrarnos a este viraje hacia la autenticidad y sin duda alguna suscitará lamentos por la privacidad perdida»[20]. Qué bien les va a Schmidt, Zuckerberg y Sandberg que estos «cambios naturales» que están registrando las normas sociales estén vinculados a sus balances personales y profesionales, ellos que se benefician directamente de monetizarte y monetizar las montañas de información que filtras en la mayor medida posible, como resultado de sus parcialísimos términos y condiciones de servicio.

No obstante, defenderse con un «No tengo nada que ocultar» es la forma más errónea de concebir la nueva sociedad de vigilancia de datos. Se trata de una falsa elección dicotómica: o aceptamos una vigilancia total o somos delincuentes que merecemos ser sospechosos. Si el argumento de los defensores del «no tengo nada que ocultar» fuera fiel a sus palabras, entonces, por pura lógica, no se opondrían a que los filmáramos mientras mantienen relaciones sexuales con sus parejas, ni a que publicáramos sus declaraciones de la renta en Internet o proyectáramos vídeos de cómo utilizan el lavabo en el Jumbotron de un estadio lleno hasta los topes, ¿no es cierto? A fin de cuentas, no tienen nada que ocultar. Pero lo cierto es que todos tenemos momentos especiales y privados en la vida, momentos que convertimos en excepcionales por el hecho de limitar con quién los compartimos.

A quienes creen en la falacia del no tener nada que ocultar, quizá les haría falta una lección en tener algo que ocultar, ya que todos nosotros preferimos no compartir determinados aspectos de nuestras vidas. Por ejemplo, Google Voice, Skype, tu operadora de telefonía móvil y varios departamentos gubernamentales guardan registros de cualquiera que haya telefoneado alguna vez a una clínica de abortos, una línea de atención a suicidas o un centro local de Alcohólicos Anónimos. Los agregadores de datos saben quién ha buscado «animadoras guarras», «Viagra» o «Prozac» en cualquiera de sus dispositivos electrónicos. Y pese a que tales comportamientos pueden ser perfectamente legales, sin duda tendrían repercusiones en nuestra sociedad si salieran a la luz.

Dado que Google y Facebook por sí solos tienen centenares de petabytes de datos acerca de sus usuarios almacenados a perpetuidad, quizá la pregunta que deberíamos formularnos no es qué tenemos que ocultar hoy, sino qué nos gustaría mantener en privado en el futuro… y, si Facebook hubiera existido en 1950, ¿cómo juzgaría la historia un chiste racista? ¿De qué delito futuro podrían acusarte sin ni siquiera saber que estabas transgrediendo la ley? ¿Cruzaste acaso la frontera de Nueva Jersey o Delaware para ahorrarte impuestos en tus compras cuando preparabas la vuelta al cole de tus hijos? Tu teléfono móvil y los extractos de tu tarjeta de crédito documentan la evasión de impuestos. Esa fotografía en Twitpic de la cena familiar en la que se ve a tu hijo de veinte años beber un vaso de vino podría ser una prueba de haber suministrado alcohol a un menor. Tal como señaló la investigadora en materia de seguridad informática Moxie Marlinspike, hay «27 000 páginas de estatutos federales» en Estados Unidos y otras «10 000 regulaciones administrativas. Probablemente sí tengas algo que ocultar, sólo que todavía no lo sabes»[21].

Riesgos para la privacidad y otras sorpresas desagradables

Tal como Mat Honan de *Wired* y el padre en duelo Mike Seay descubrieron, nuestros datos personales pueden acabar en manos de personas que seguramente preferiríamos que no tuvieran acceso a tal información. La combinación de nuestros datos sociales con bases de datos públicas, balizas y localizaciones pueden desembocar en una serie de consecuencias insospechadas e incluso peligrosas. Dicho de otra manera, tus datos son cada vez más promiscuos. Fluyen de un sistema a otro, de una base de datos a otra, y son distribuidos entre sombras a redes basadas en la nube de todo el mundo, compartidos, procesados y vendidos. No obstante, tal como hemos aprendido del mundo real, la promiscuidad a menudo puede provocar enfermedades sociales y otras consecuencias imprevistas.

En un incidente no muy distinto a la debacle de OfficeMax, un hombre de Mineápolis supo que su hija estaba embarazada, pero no por boca de ella, sino a través de un comercio local, Target. Lo descubrió cuando Target empezó a enviar a la muchacha de quince años cupones para artículos que su padre desaprobaba. Armado con dichos cupones de descuento y una carta dirigida a su hija, el padre se plantó enfurecido en la tienda y empezó a amonestar al encargado. «¡A mi hija le ha llegado esto al buzón! […] Aún está en el instituto ¿y ya le están enviando descuentos para ropa de bebé y cunas? ¿Es que pretenden alentarla a que se quede embarazada?»[22]. Días después, el hombre telefoneó a la tienda para disculparse alegando que «En mi casa han estado sucediendo algunas actividades de las cuales yo no estaba al tanto. Espera un bebé en agosto. Les debo una disculpa». Pero ¿cómo diablos supo Target que la muchacha estaba embarazada? Mediante su algoritmo de predicción de embarazos, por supuesto, que agregaba todo el historial de compras de un cliente a las estadísticas demográficas adquiridas a los agentes intermediarios de datos. Target pensó que, si daba con esas mujeres antes del segundo trimestre del embarazo y lograba captarlas como clientas, se llevaría la mayor tajada del pastel de sus compras, no sólo en lo tocante a toallitas para bebés, cunas y pañales, sino también los juguetes y la ropa que los pequeños fueran necesitando desde la más tierna infancia hasta el final de su adolescencia. A raíz de un estudio en profundidad efectuado por los estadistas de la empresa, Target supo que las mujeres embarazadas «compraban mayores cantidades de loción sin perfume al principio de su segundo trimestre, además de suplementos de vitaminas, como calcio, magnesio y zinc». En total, Target fue capaz de identificar veinticinco productos que, analizados en conjunto, le permitieron asignar a cada cliente un «marcador de predicción de embarazo». Cuando se cotejó dicho modelo con los millones de mujeres incluidas en las bases de datos de clientes de Target, se identificó a miles y miles de embarazadas antes de que ninguna otra empresa hubiera establecido tal conexión. Target y los comerciantes de la empresa estaban embelesados con aquel descubrimiento. Menos fascinado estuvo el padre de aquella joven de quince años de Mineápolis que descubrió que esperaba un nieto a través de un folleto de vales de descuento depositado en su buzón. Y teniendo en cuenta el ataque pirata informático de Target en 2013, como parte del cual se revelaron los datos económicos de 110 millones de sus clientes, ¿qué garantías tienen los consumidores de que los enormes tesoros adicionales de datos sumamente personales que Target pueda tener almacenados en sus criptas no serán sustraídos algún día[23]? ¿Pueden los clientes confiar en Target o en cualquier otra cadena gigante de comercios con los volúmenes de datos que recopila, almacena y analiza? Probablemente no, y ahí radica el problema.

Ahora bien, nuestros datos personales no sólo corren riesgos en manos de los piratas informáticos, sino que, como cada vez más personas descubren, también en las de las analíticas de *big data* o datos masivos. Previamente, muchos de los datos agregados permanecían en una especie de limbo, pues nuestras capacidades de

recopilación sobrepasaban nuestra habilidad para entender todo lo que se había recopilado. Sin embargo, eso está cambiando en el presente y los datos que filtramos en redes sociales como Facebook nos muestran de cara a los demás de modos insospechados. Una de esas personas afectadas fue Bobbi Duncan, una estudiante lesbiana de veintidós años de la Universidad de Texas, en Austin. Procedía de una familia cristiana estricta y se había esforzado muchísimo por ocultar su orientación sexual a sus padres. A medida que fue entendiéndose mejor, se unió a diversos grupos de estudiantes en el campus universitario, incluido entre ellos el Queer Chorus, con el fin de conocer a otros alumnos homosexuales en la universidad. Cuando se inscribió en la organización, el presidente del Queer Chorus dio la bienvenida a Bobbi añadiéndola al foro de discusión del grupo en Facebook, cosa que pudo hacer sin el permiso de la implicada, pues no existe ningún ajuste en Facebook que impida a un tercero añadirte a su grupo. Al hacerlo, Facebook envió una notificación de sistema automática a toda la lista de amistades de Bobbi, incluido su padre, indicándoles que se había inscrito en el Queer Chorus. Dos días después de recibir la notificación, el padre de Bobbi escribió una respuesta en su página de Facebook: «A todos vosotros, homosexuales. Regresad a vuestras madrigueras y esperad a DIOS. El infierno os espera, pervertidos. Que os lo paséis bien cantando allí». Facebook sacó del armario a una lesbiana e hizo que sus padres la repudiaran. En respuesta al daño irreparable que había sufrido, Bobbi fue inequívoca en su declaración: «Culpo de lo ocurrido a Facebook […] Nadie, aparte de mí misma, debería escoger qué información sobre mí se muestra públicamente»[24].

Cuando se es la mercancía de empresas de Internet y redes sociales, el desafío que se afronta es que los datos que has proporcionado en un contexto puedan ser utilizados de modos insospechados en otro, con consecuencias notables. Tal es el caso del célebre sitio web «gratuito» de citas OkCupid. En él se solicita a los usuarios que buscan pareja que rellenen cuestionarios, y la mayoría de ellos dan por sentado, equivocadamente, que los datos que aportan se circunscriben al sistema de OkCupid y se utilizan exclusivamente para encontrarles una pareja idónea con quien tener una cita. ¡Qué más quisieran ellos! Para, supuestamente, conseguir las mejores citas, OkCupid formula a los usuarios un montón de preguntas personales, como son el número de parejas sexuales en el pasado, si están a favor o en contra del derecho al aborto, si poseen un arma de fuego, si se acostarían con alguien en la primera cita, si fuman cigarrillos y si beben alcohol con frecuencia o consumen drogas ilegales (inclusive qué drogas y con qué frecuencia). Al menos eso es lo que los usuarios ven en sus perfiles cuando los rellenan…

Lo que no ven son las cincuenta y tantas empresas con las que OkCupid comparte esta información, incluidas empresas publicitarias, agentes intermediarios de datos y comerciantes. Para entender el alcance de la filtración de datos, Ashkan Soltani, un especialista en privacidad digital que antiguamente trabajaba en la Comisión Federal de Comercio, creó una cuenta falsa en OkCupid. Sirviéndose de varias herramientas

para ajustar la privacidad del navegador, módulos *plug-in* gratuitos, como Collusion y mitmproxy, Soltani logró observar que las respuestas proporcionadas por los usuarios de OkCupid se analizaban y enviaban a docenas de agentes intermediarios de datos en tiempo real. Cuando Soltani completó su perfil de prueba en OkCupid e indicó que consumía drogas con frecuencia, logró observar cómo un archivo *cookie* que compartía la información sobre su supuesto consumo de drogas era enviado a un agente intermediario de datos conocido como Lotame. Uno piensa que simplemente está rellenando un perfil confidencial en un servicio de citas online «gratuito», cuando, en realidad, está detallando información sobre sí mismo que de otro modo jamás compartiría con ninguna empresa de mercadotecnia o agente intermediario de datos. Es un ardid de los grandes: encontrar pareja es sólo «la fachada» para proceder a una extracción masiva de datos. En la investigación que Soltani procedió a realizar para NPR, tanto OkCupid como Lotame se negaron a realizar declaraciones sobre este asunto[25]. Tal es el estado de la cuestión en el sector internacional no regulado de los agentes intermediarios de datos. ¿A quién más podría interesarle pagar por el archivo de OkCupid relativo a tu consumo de drogas e historial sexual? Pues a una empresa aseguradora, a posibles empleadores futuros o quizá al gobierno tras un incidente de conducción bajo la influencia del alcohol que tuviste el pasado junio.

Aun cuando no se tiene «nada que ocultar», el gráfico de tu red social, que se rastrea de manera continua, y tu localización pueden volverse en tu contra y afectar incluso a tu situación económica. Un puñado de *start-ups* del ámbito de la tecnología han empezado a utilizar la calidad de tus amigos en tu red social para determinar si eres una persona de confianza con vistas a concederte un crédito[26]. Una de dichas empresas, Lenddo, determina si eres amigo de alguien que va retrasado en los pagos de su préstamo y con qué frecuencia interactúas con esa persona. Como resultado de ello, tu adecuación para solicitar un crédito puede menguar debido a tus amistades en Facebook. Y si tus amigos en Google+ y Pinterest son unos vagos, lo más probable es que tú también lo seas (según los dioses de los datos masivos). Facebook podría convertirse en el siguiente organismo de clasificación de créditos FICO, si los agregadores de datos económicos aprovechan todas las ventajas que aportan tus publicaciones en redes sociales para determinar tu estabilidad económica[27]. Así que, como te advertía tu mamá con sabio criterio, escoge bien a tus amistades.

El hecho es que todos contribuimos a nuestra propia contaminación digital. Del mismo modo que las personas del siglo XX no se planteaban si verter residuos industriales a un río o tirar basura a la calle tenía repercusiones, nosotros tampoco entendemos las consecuencias a largo plazo de nuestras acciones digitales de hoy. La situación presente se debe a nuestra falta de comprensión fundamental en torno al trato que hemos aceptado a cambio de los llamados servicios online gratuitos.

Abrir la caja de Pandora virtual

Las personas comparten sus pensamientos y secretos más íntimos en Internet como si estuvieran manteniendo una conversación privada con un amigo de confianza. Y ojalá el sistema legal las amparara. En Estados Unidos, las redes sociales se consideran espacios públicos, no privados, y cualquier información que se comparta en ellas queda cubierta por la llamada doctrina de terceras partes, que, simple y llanamente, significa que los usuarios no deben esperar que los proveedores de servicios (las operadoras de telefonía móvil, proveedores de servicios de Internet, compañías por cable y sitios web) traten con privacidad los datos que recopilan acerca de ellos[28].

Esta notable excepción a la prohibición de búsquedas y decomiso irrazonables de la Cuarta Enmienda implica que todos los datos que publicas online, en cualquier formato (al margen de los ajustes de privacidad que tengas configurados) y todos los datos recopilados por las terceras partes con quienes has establecido una relación empresarial al aceptar sus términos y condiciones no se consideran privados. Y tampoco se ajusta al principio constitucional de «documentos privados», sino que forma parte de los registros empresariales de la institución propietaria de los datos. Por chocante que pueda resultar, tal es la situación actual de la jurisprudencia en Estados Unidos, con un impacto notorio y profundo en todos los ciudadanos, tanto los que están conectados en red como los que no. De ahí que tus datos se filtren a destinos que nunca serían de tu interés y que no puedas recuperarlos, por mucho que te esfuerces.

En la misma línea, la palabra «Facebook» apareció en un tercio de las peticiones de divorcio de 2011[29]. Todo esto proporciona un pasto excelente al 81 por ciento de los abogados de divorcios, quienes admiten recabar pruebas en las redes sociales para esgrimir en contra del cónyuge de sus clientes. Por ejemplo, todos los datos compartidos en Facebook y Twitter y todos los registros telefónicos del móvil y datos de localización del GPS que emitieron aquellas personas cuyo móvil se hallaba junto al del demandante pueden convertirse en juego limpio en esa batalla monumental que puede ser un juicio de divorcio. Las fotografías que de manera inocente te sacaron en todas esas fiestas a lo largo de los años, con la mirada perdida y una copa en la mano, pueden así convertirse en pruebas de no ser un padre apto, una pepita de oro para el abogado de la oposición durante el turno de preguntas. Y ese perfil que creaste en OkCupid indicando que eras soltero (y que mediante las *cookies* de tu navegador se compartió con cincuenta empresas de *marketing*) se considerará perfectamente admisible cuando tu esposa lo presente en la vista para el divorcio. Cuando un marido se queja de que su mujer es una madre inadecuada que no presta la suficiente atención a sus vástagos, ahora cuenta con una potente prueba para respaldar sus afirmaciones, en la forma de los registros citatorios que documentan los cientos de horas que ha estado conectada a *FarmVille* y *World of Warcraft*, horas que coinciden

con los partidos de fútbol o béisbol de sus hijos a los que no ha asistido. Ahora bien, los datos que filtramos no sólo nos afectan durante los procesos de divorcio, sino que también pueden tener repercusiones laborales.

Una encuesta realizada por Microsoft en torno al tema de la reputación en Internet desveló que el 70 por ciento de los profesionales del ámbito de los recursos humanos habían rechazado a un candidato para un empleo basándose en la información que habían obtenido durante sus pesquisas en Internet[30]. Peor aún, algunos empresarios exigen ahora las contraseñas de sus perfiles en las redes sociales a los solicitantes de un empleo e incluso a sus empleados en nómina. Si quisieras trabajar para Norman en Oklahoma, el Departamento de Policía, el Departamento de Seguridad Pública y los Servicios Correccionales de Maryland, el Ayuntamiento de Bozeman, Montana, o para la Policía del estado de Virginia, estarías obligado a entregar tus contraseñas de Facebook y otras redes sociales como parte de las llamadas «comprobaciones de fondo rutinarias»[31]. Esto supone entregar a tus posibles empleadores futuros acceso a todos tus mensajes, fotografías, cronologías y publicaciones en el muro, tanto privados como públicos, en Facebook, Google, Yahoo!, YouTube e Instagram. Mientras que algunos estados, incluida California, han prohibido tales prácticas contra el personal, no existe ninguna ley federal que las prohíba y siguen siendo legales en el 80 por ciento de los estados norteamericanos, con la consiguiente filtración de datos[32].

Cada vez son más los profesores y escuelas públicas que solicitan esta información también a sus alumnos, sin orden judicial, por supuesto. Eso fue lo que le sucedió a una alumna de secundaria de doce años de Minnesota, a quien acusaron de publicar «comentarios inadecuados» en su cuenta de Facebook[33]. La estudiante de la escuela de secundaria Minnewaska Area Middle School había publicado que «odiaba» a un empleado de una escuela particular que «le tenía manía». La niña fue requerida en la oficina del director, donde varios administradores, un psicólogo infantil y un ayudante del *sheriff* la estaban esperando y le exigieron que les revelara su contraseña de Facebook para poder revisar todas sus publicaciones. Y sí, por supuesto que hay una demanda judicial en curso, pero el número creciente de casos indignantes demuestra que nuestros hijos también filtran datos que pueden volverse en su contra.

Incluso a los deportistas universitarios de instituciones como la Universidad de Carolina del Norte y la Universidad de Oklahoma se les exige ahora que proporcionen sus contraseñas a las redes sociales a sus entrenadores como condición para jugar con sus equipos[34]. A algunos deportistas universitarios también se les ha obligado a instalar *software* de monitorización en sus ordenadores y teléfonos personales, programas creados por empresas como UDiligence que rastrean las actividades de los alumnos en tiempo real para garantizar «la protección de los departamentos deportivos colegiados de las publicaciones realizadas por alumnos deportistas».

Los gobiernos también se están poniendo manos a la obra. Una encuesta realizada por la Asociación Internacional de Jefes de Policía de más de quinientas organizaciones de cuerpos policiales reveló que el 86,1 por ciento de los departamentos policiales incluyen actualmente de manera rutinaria búsquedas en las redes sociales como parte de sus investigaciones criminales[35]. También la IRS (Agencia Tributaria estadounidense) comenzó a formar a sus investigadores acerca de cómo utilizar las redes sociales para investigar a los contribuyentes en 2009, y el servicio de Inmigración y Ciudadanía del Departamento de Seguridad Nacional de Estados Unidos instruyó a sus agentes en 2010 para que utilizaran las redes sociales con el fin de «observar la vida diaria de los demandantes y beneficiarios sospechosos de fraude»[36].

Los agentes federales pueden acceder a su antojo a nuestros datos en las redes sociales mediante una serie de métodos, ya sea presentando citaciones, cartas de seguridad nacional u otras órdenes administrativas a los proveedores de servicios, quienes, gracias a la excepción doctrinaria de terceras partes a la Cuarta Enmienda, ni siquiera necesitan notificarte su solicitud. Sin ir más lejos, AT&T reveló que en 2013 había recibido más de 300 000 solicitudes de datos relacionados tanto con casos civiles como delictivos. Las peticiones de información procedían de autoridades estatales, federales y locales e incluían cerca de «248 000 citaciones, en torno a 37 000 órdenes judiciales y más de 16 000 órdenes de registro»[37]. En 2009, *Sprint* reveló que incluso había creado un portal para los cuerpos de seguridad, el cual otorgaba a la policía la capacidad de «pinchar» (sin orden judicial previa) cualquier teléfono móvil de *Sprint* para poder geolocalizar a los usuarios a tiempo real, una función que la policía empleó más de ocho millones de veces en sólo un año de plazo[38].

Y aquellos datos que el gobierno no obtiene mediante citación, se limita a comprarlos. La NSA y otros organismos gubernamentales no han construido su red de extracción de datos y escuchas ilegales mundial a partir de cero; adquirieron u obtuvieron por otros medios una copia completa de lo que el mundo corporativo ya tenía almacenado. Y es que es lo más lógico: ¿por qué construir algo si pueden comprarlo[39]? ChoicePoint, actualmente propiedad de Reed Elsevier, mantiene diecisiete mil millones de registros sobre empresas y personas que revende a sus cien mil clientes, incluidos entre ellos siete mil organismos de las fuerzas de seguridad federales, estatales y locales de Estados Unidos. Las revelaciones realizadas por Edward Snowden alegaban que la CIA (Agencia de Inteligencia Central) paga a AT&T diez millones de dólares anuales por sus datos de llamadas y sugería que Verizon también suministra datos al gobierno estadounidense[40]. Los agentes intermediarios de datos comerciales no han perdido el tiempo a la hora de ofrecer sus servicios de suscripción de pago a organismos gubernamentales, a quienes proporcionan flujos de información que les hemos suministrado de manera gratuita a través de las redes sociales.

Una parodia brillante en la cadena cómica Onion News Network satirizaba el estado actual de la cuestión con una noticia falsa de un telediario nocturno:

> El Congreso ha vuelto a dar luz verde hoy a la financiación de Facebook, el programa de vigilancia online masiva dirigido por la CIA. Según se informa, Facebook ha reemplazado a prácticamente todos los programas de recopilación de información de la CIA desde su lanzamiento en 2004. [Un falso oficial de la CIA declaraba:] «Tras años de monitorizar en secreto al público, nos dejó perplejos que tantas personas estuvieran dispuestas a desvelar por voluntad propia dónde viven, cuáles son sus opiniones políticas y creencias religiosas, un listado alfabetizado de sus amistades, direcciones personales de correo electrónico, números telefónicos, cientos de fotos de sí mismas e incluso actualizaciones de estado en las que indicaban qué estaban haciendo en cada momento. Para la CIA, es un sueño hecho realidad. Gran parte del crédito se debe al agente de la CIA Mark Zuckerberg, quien dirige las operaciones cotidianas de Facebook para la agencia»[41].

Por hilarante a la par que certera que fuera aquella noticia falsa, la filtración de nuestros datos personales a agentes intermediarios en la sombra y organismos gubernamentales no es ninguna broma. El coste de la economía de la vigilancia, en gran medida debido a los avances tecnológicos, desciende de manera exponencial. Ya no es preciso mantener enormes equipos de agentes especiales que te sigan a todas partes, a pie o en vehículo, mientras atraviesas la ciudad. En su lugar, un estudio ha calculado que mediante tecnologías de vigilancia intermediarias, como los teléfonos móviles, la actividad en Internet, los datos de las redes sociales, la información del GPS y las transacciones económicas, el gobierno invierte ahora sólo «574 dólares por contribuyente, unos irrisorios 6,5 centavos por hora» en realizar el seguimiento de cada estadounidense[42].

Al conocer el verdadero alcance de la capacidad de espionaje tanto internacional como doméstico de la NSA, el exdirector de las Stasi de la Alemania del Este, Wolfgang Schmidt, admitió públicamente que un sistema así «habría sido un sueño hecho realidad»[43]. Schmidt destacó que durante su etapa como director del temido servicio de la policía secreta de la antigua República Democrática Alemana, la Stasi únicamente tenía capacidad para pinchar cuatro teléfonos nacionales de manera simultánea, mientras que la tecnología actual claramente había hecho posible monitorizar todas las llamadas y datos de Internet de manera constante. Y advertía: «El colmo de la ingenuidad sería pensar que, una vez recopilada, esa información no se utilizará. […] Tal es la esencia de las organizaciones gubernamentales secretas. El único modo de proteger la privacidad de las personas es no permitir que el gobierno recopile su información».

El conocimiento es poder, el código es el rey y Orwell tenía razón

En la novela distópica de George Orwell *1984*, el autor describía un estado de vigilancia gubernamental omnipotente controlado por una élite privilegiada integrada por unas cuantas personas que perseguían el pensamiento independiente por considerarlo «crimen de pensamiento». Pese a que Orwell sin duda alguna habría barruntado la debacle de la NSA, no está tan claro que hubiera predicho la existencia de Acxiom, Facebook y Google. Y es que en estos casos no podemos acusar a un gobierno al estilo del Gran Hermano de «habernos hecho nada», sino que los agentes hemos sido nosotros mismos. Hemos permitido que nos pongan un precio y nos conviertan en una mercancía, y lo hemos hecho de manera gratuita, regalando miles de millones de dólares por nuestros datos personales a nuevas élites que atisbaron una oportunidad y la aprovecharon. Aceptamos todos sus términos de servicio unilaterales sin detenernos siquiera a leerlos y ellos maximizan sus beneficios, sin que ninguna regulación o supervisión les ponga trabas. Cierto, hemos conseguido algunos productos interesantes a cambio, y *Angry Birds* es realmente divertido. Pero ahora que hemos regalado todos esos datos nos encontramos a expensas de poderosos mastodontes de datos con un poder similar al de cualquier gobierno para hacer lo que les plazca con nuestra información y nuestras vidas.

En su libro de 1999, *El código y otras leyes del ciberespacio*, el profesor de la Facultad de Derecho de Harvard Lawrence Lessig demostraba con conocimiento de causa que las instrucciones codificadas en un programa informático, aplicación o plataforma conforman y delimitan Internet, de la misma manera que lo hacen las leyes y regulaciones. Así, cuando Facebook o Google modifican de manera unilateral sus términos de servicio para permitir que tus publicaciones en el muro sean públicas o utilizar tus fotografías en publicidad contra tu voluntad, equivaldría a aprobar una nueva «ley». El código, en efecto, es la ley.

Por consiguiente, quizá el único modo de salirse de este sistema sería cerrar la cuenta para siempre o, mejor aún, no crearla, ¿no es cierto? Por desgracia, ambos planteamientos son problemáticos y cada vez más imposibles. Un artículo del *New York Times* explicaba que Facebook conserva todos tus datos incluso después de cerrar tu cuenta[44]. Y aunque decidas no participar en ninguna red social en línea, tus amigos te seguirán etiquetando en fotografías, el GPS de tu coche seguirá informando de tu localización y la red de comercios Target monitorizará todas tus compras.

Los volúmenes sin precedentes de datos acerca de nosotros mismos que hemos cedido a empresas privadas están al alcance de cualquiera y, una vez el genio sale de la lámpara, es imposible encerrarlo de nuevo. La *troika* de la oportunidad creada por nuestra estela de datos online, los ridículos términos y condiciones de servicio y la escasa o nula regulación implican que los agentes intermediarios de datos modernos pueden vigilarnos gracias a métodos de vigilancia incluso mejores que los del gobierno, registrar nuestros pensamientos, fotografías y ubicaciones, y someterlos a análisis de datos masivos. Tal como Mat Honan, Bilal Ahmed, Mike Seay, Bobbi Duncan, Leigh Van Bryan y Emily Bunting averiguaron de primera mano, nuestra

filtración constante de datos lleva asociada una serie de costes y riesgos. Sin embargo, las implicaciones para la privacidad son sólo una de las grandes amenazas derivadas del crecimiento exponencial de datos.

Los *hackers* se apresuran a robar todos los datos que has proporcionado debidamente en las redes sociales y consiguen abrirse camino en los ordenadores de los agentes intermediarios de datos y gigantes de Internet que se encargan de almacenarlos. Como Sony, Target e incluso del Departamento de Defensa de Estados Unidos han aprendido, los datos almacenados en sistemas de información inseguros pueden ser hurtados en cualquier momento. Como tal, todos los datos recopilados en un momento u otro acabarán filtrándose, con potentes repercusiones tanto para nuestra vidas personales como profesionales e incluso para nuestra seguridad.

El problema de que nosotros seamos la mercancía en lugar del cliente de los agentes intermediarios de datos masivos es que no tenemos el control sobre nuestros datos y, por consiguiente, hemos perdido las riendas de nuestro destino. La acumulación incesante de información desregulada e insegura es una bomba de relojería, y nuestros pensamientos y actos están expuestos a que los robe una nueva clase emergente de agentes maléficos cuyas intenciones son mucho peores que vendernos pañales con descuento o ajustar la tarifa de nuestro seguro médico. Grupos de la delincuencia organizada internacional, gobiernos corruptos e incluso terroristas se apremian a establecer sus propios intermediarios de datos y refuerzan sus capacidades analíticas con el fin de sacar el máximo partido a la mayor bonanza que se les ha cruzado nunca en el camino, con implicaciones que nos harían echarnos a temblar.

Capítulo 6

Datos masivos, riesgos masivos

> Nuestro poderío tecnológico aumenta, pero los efectos secundarios y los riesgos potenciales también son cada vez más elevados.
>
> ALVIN TOFFLER

La noche del 26 de noviembre de 2008, un hombre de sesenta y nueve años se registró en la habitación 632 del lujoso hotel Taj Mahal Palace en Bombay, India. El huésped, K. R. Ramamoorthy, procedente de Bangalore, se hallaba en la ciudad en un viaje de negocios rutinario. Poco sabía que su vida estaba a punto de cambiar para siempre.

En torno a las 23:00 horas, Ramamoorthy escuchó un breve alboroto al otro lado de la puerta y, de repente, alguien llamó con los nudillos. «Servicio de habitaciones», anunció una voz. Ramamoorthy sabía que no había encargado nada y tuvo el presentimiento de que algo iba terriblemente mal. Intentó esconderse en el cuarto de baño, con la mala fortuna de que tropezó con la puerta. El ruido delató su presencia en la habitación del hotel. La respuesta no se hizo esperar: una ráfaga de balas atravesó la puerta e hizo añicos la cerradura que separaba a aquel hombre de negocios del mundo exterior.

Dos hombres armados hasta los dientes irrumpieron en la habitación de Ramamoorthy y, en un abrir y cerrar de ojos, lo habían apaleado, desnudado y atado, en la que se convertiría en la noche más aterradora de su vida. Los hombres pertenecían a la organización terrorista afiliada a Al Qaeda y con base en Pakistán conocida como Lashkar-e-Toiba (LeT), y Ramamoorthy tuvo la desgracia de hallarse en el epicentro del mortal asedio terrorista que la ciudad de Bombay sufrió en 2008.

«¿Quién es usted y qué hace aquí?», le preguntaron sus captores de LeT. «Sólo soy un inocente maestro de escuela», respondió Ramamoorthy. Por supuesto, los terroristas sabían que ningún maestro de escuela indio podía permitirse alojarse en una *suite* en el hotel más opulento de la ciudad. Los terroristas localizaron el carnet de identidad de su rehén en la mesilla de noche y así conocieron su verdadero nombre, que transmitieron a los comandantes terroristas a través del teléfono satélite que llevaban consigo.

El centro de operaciones de LeT que recibió la llamada recordaba a cualquier instalación de mando y control militar actual. Desde el otro lado de la frontera en Pakistán, los líderes de la célula terrorista llevaban un seguimiento de su ataque contra la población de Bombay. Habían seleccionado sus objetivos con esmero: dos

hoteles de lujo, una concurrida estación ferroviaria, un centro comunitario judío, una cafetería muy turística e incluso un hospital para mujeres y niños. En el terreno de Bombay, los terroristas lanzaron sin piedad granadas de mano a personas inocentes que disfrutaban de un café en la cafetería y tirotearon a civiles desarmados que esperaban a sus trenes para regresar a sus hogares tras la jornada laboral.

A medida que los atentados iban perpetrándose, los comandantes de LeT en Pakistán utilizaron su sala de guerra para supervisar atentamente las emisiones de la BBC, Al Jazeera, la CNN y las cadenas locales de la televisión india con el fin de recabar la máxima información posible acerca del progreso de sus agentes y la respuesta del gobierno indio. Por desgracia, los terroristas no limitaron sus operaciones de obtención de información a los medios de comunicación, sino que también minaron Internet y las redes sociales en tiempo real, con repercusiones letales.

Cuando los terroristas que retenían a Ramamoorthy comunicaron su nombre a la base pakistaní, el centro de operaciones efectuó una búsqueda en Internet para saber quién era su rehén. Instantes después tenían su fotografía. Luego supieron su lugar de trabajo. Descubrieron así que Ramamoorthy no era un inocente maestro de escuela que suplicaba por su vida, sino el director de uno de los principales bancos de India, ING Vysya. Basándose en la imagen que habían encontrado en Internet, los mandos terroristas solicitaron a sus operativos en el Taj Mahal Palace que compararan al hombre que tenían delante con la fotografía del presidente del banco que había en línea:

—¿El rehén es un hombre fornido?
—Sí.
—¿Tiene calva frontal?
—Sí.
—¿Lleva gafas?
—Sí.
—¿Qué hacemos con él? —preguntaron los captores de Ramamoorthy.

Momentos después, la sala de guerra terrorista dio su respuesta: matarlo. En un instante, una simple búsqueda en Internet fue todo lo que los terroristas necesitaron para decidir el destino de aquel anciano. Y por mucho que nos preocupe que los anunciantes y los agentes intermediarios de datos se salten a la torera los ajustes de privacidad que tenemos configurados en Facebook, lo que de verdad importa es que nuestra franqueza puede irnos a la contra más de lo que jamás hemos imaginado. Cuando filtramos datos, no sólo los captan empresas y gobiernos. Los delincuentes y terroristas también tienen acceso a nuestras redes sociales y lo están utilizando con una precisión asesina. En el mundo actual, un motor de búsqueda puede determinar, literalmente, quién debe vivir y quién morir.

Los hombres que perpetraron los atentados en Bombay iban armados con AK-47 y explosivos RDX. Las armas y bombas no son elementos nuevos en las operaciones

terroristas, pero aquellos agentes de LeT representaban una nueva raza de terrorista, y es espeluznante. Habían visto el futuro y emplearon las tecnologías de la información modernas en cada paso que dieron durante su asalto para localizar y masacrar a las víctimas.

Cuando los atacantes zarparon al mar desde Pakistán bajo el manto de la noche, iban equipados con gafas de visión nocturna, y se desplazaron hasta Bombay con la ayuda de un GPS de mano. Portaban BlackBerrys con archivos PDF de los planos de las plantas de los hoteles y utilizaron Google Earth para estudiar maquetas tridimensionales de los recintos que se habían marcado como objetivos, con el fin de determinar cuáles eran los puntos de entrada y salida óptimos. Durante el tumulto, los asesinos de LeT utilizaron teléfonos vía satélite, GSM de mano y Skype para coordinarse con su centro de mando ubicado en Pakistán, que monitorizó las noticias en los medios de comunicación, Internet y las redes sociales para proporcionar instrucciones tácticas a tiempo real a su equipo de asalto sobre el terreno.

Cuando un transeúnte tuiteó una fotografía de los comandos policiales descendiendo en rápel desde un helicóptero hasta el tejado del edificio de la comunidad judía asediado, el centro de operaciones terrorista interceptó la imagen, alertó a sus hombres y los dirigió hasta una escalera que conducía al tejado. Los policías, que esperaban tomar a los terroristas por sorpresa, acabaron siendo víctimas de una emboscada en la escalera en cuanto abrieron la puerta. Y cuando la BBC mencionó en directo que los testigos habían informado de que los terroristas se ocultaban en la habitación 360 o 361, la sala de guerra los telefoneó al instante y les advirtió que se reubicaran para evitar ser apresados.

En todo momento durante el ataque, los terroristas de LeT se sirvieron de tecnologías al alcance de todos para obtener datos de la situación y mantener una ventaja táctica frente a la policía y el gobierno. Monitorizaron Internet y las redes sociales, recabaron todos los datos de código abierto disponibles e incluso montaron una sofisticada operación de contrainteligencia online para proteger a sus operativos. Durante todo su asalto a Bombay, los terroristas dependían en tal medida de la tecnología que numerosos testigos afirmaron haber visto a los operativos de LeT disparar a los rehenes con el arma en la mano derecha al tiempo que comprobaban los mensajes en sus BlackBerry con la izquierda.

La tecnología no sólo fue crucial para el éxito operativo del ataque, sino que, tal como hemos visto en el capítulo 2, el uso indebido que los delincuentes hacen de la ella también permitió financiar el ataque. Una célula de piratas informáticos filipina que trabajaba en nombre de la filial de Al Qaeda Jemaah Islamiya cometió un ciberdelito y fraude en línea masivo para aportar los fondos de la operación de LeT en la India. Los *hackers* canalizaron sus millones de ciberganancias obtenidas de manera ilícita hasta sus gestores en Arabia Saudía, quienes, a su vez, blanquearon los fondos y los remitieron al equipo de Lashkar-e-Toiba responsable de la brutal matanza contra la población de Bombay[1].

Al final, la policía tardó sesenta y ocho horas en poner fin al asedio de la ciudad de Bombay. Los equipos de contraataque acabaron matando a nueve de los terroristas y arrestaron al décimo. Asombrosamente, uno de los inocentes que sobrevivió al atentado fue K. R. Ramamoorthy. En el mismo momento en el que el centro de mando de LeT había dado la orden de matarlo se produjo una explosión en el Taj Mahal Palace y los terroristas creyeron que la policía venía a por ellos. Cuando salieron corriendo a investigar qué sucedía, concedieron a Ramamoorthy los breves instantes que necesitó para liberarse y escapar. No tuvieron tanta suerte los 166 hombres, mujeres y niños que perdieron la vida aquel día, ni tampoco los cientos de personas que resultaron gravemente heridas en aquella masacre.

Hagamos una pausa unos instantes para analizar las implicaciones de este ataque terrorista. Diez hombres, armados no sólo con armas, sino también con tecnología, fueron capaces de paralizar por completo una ciudad de doce millones de habitantes, la cuarta mayor metrópolis del mundo, en un acontecimiento que se retransmitió en directo en todo el planeta. Los militantes terroristas demostraron ser plenamente capaces de recopilar datos de inteligencia de código abierto en pleno ataque (mediante los medios de comunicación tradicionales, Internet, los móviles y las redes sociales) y usarlos para adoptar decisiones operativas de manera sincrónica. LeT se limitó a procesar los datos que el público iba filtrando y los utilizó en tiempo real para matar a más personas y aventajar a las autoridades. Ése era el terrorismo en la era digital en torno a 2008. ¿Qué podrían hacer los terroristas con las tecnologías disponibles hoy en día? ¿Qué harán con las tecnologías del mañana? La lección de Bombay es que los cambios exponenciales no sólo se aplican para bien, sino también para mal.

Los datos son el petróleo de hoy en día

Todo a nuestro alrededor genera datos de manera constante. Todo proceso digital, sensor, teléfono móvil, dispositivo GPS, motor automovilístico, análisis de laboratorio médico, transacción con tarjeta de crédito, apertura o cierre de una puerta de hotel, boletín de notas de la escuela e intercambio en las redes sociales genera datos. Los teléfonos móviles están convirtiendo a los seres humanos en sensores humanos y forjan inmensas cantidades de información sobre nosotros. Como resultado de ello, los niños nacidos en el presente vivirán todas sus vidas a la sombra de una inmensa huella digital[2]. El 92 por ciento de los bebés ya tienen presencia en Internet. Desde la publicación de sus padres del primer sonograma en el útero hasta la desconexión de su marcapasos activado por Internet más de cien años después, cada momento desde su vida hasta su muerte quedará registrado digitalmente y se conservará en la nube hasta la eternidad. El ciclo de generación de datos no descansa

nunca. En 2014, cada minuto de nuestras vidas:

- enviamos 204 166 667 mensajes de correo electrónico,
- efectuamos dos millones de consultas en el motor de búsqueda de Google,
- compartimos 684 000 piezas de contenido en Facebook,
- publicamos 100 000 tuits en Twitter,
- descargamos 47 000 aplicaciones de la tienda App Store de Apple,
- publicamos 48 horas de vídeo nuevo en YouTube,
- publicamos 36 000 fotografías nuevas en Instagram y
- enviamos 34 millones de mensajes por WhatsApp[3].

Dicho de otro modo, cada diez minutos creamos la misma información generada por las primeras diez mil generaciones de seres humanos[4]. Además, el coste de almacenar todos estos datos desciende en picado[5]. Por ejemplo, a finales de 2014 podía adquirirse un disco duro de 6 TB en Amazon.com por sólo 300 dólares y guardar en él toda la música grabada en todo el mundo a lo largo de toda la historia.

Esta inmensa evolución de la infraestructura de la información mundial se ha bautizado como la «revolución de los datos masivos». La promesa de los datos masivos es que los problemas complejos de larga trayectoria devienen cuantificables y, por ende, pueden resolverse de manera empírica. Piensa, por ejemplo, en la medicina. Conforme los datos de todos los pacientes van catalogándose en registros médicos electrónicos, a los médicos les resulta cada vez más fácil explorar esas bases de datos para identificar los tratamientos más eficaces, detectar interacciones de medicamentos letales e incluso predecir el brote de una enfermedad antes de que empiecen a manifestarse sus primeros síntomas físicos. Podrían salvarse incalculables vidas.

En todos los sectores, ya sea en el del comercio minorista, el transporte o las farmacéuticas, el valor económico resultante de los datos masivos será tremendo, tanto como para que el Foro Económico Mundial haya afirmado recientemente que los datos son «el petróleo de hoy en día»[6]. Hay una nueva fiebre del oro en marcha, con cientos de empresas, como IBM, Oracle, SAS, Microsoft, SAP, EMC, HP y Dell, organizándose de manera agresiva para maximizar los beneficios que pueden obtener de este fenómeno de los datos masivos. Y si los datos son el nuevo petróleo, la divisa actual en el mundo digital, entonces quienes los posean en mayor cantidad tendrán un poder y una influencia sensacionales. De la misma manera que los primeros barones del petróleo, como John D. Rockefeller y J. Paul Getty, gobernaron su era, pronto lo harán quienes posean las mayores cantidades de datos en el mundo actual, tal como han demostrado Mark Zuckerberg y Eric Schmidt. Empresas como Facebook, Google y Acxiom están componiendo los conjuntos de datos más voluminosos acerca del comportamiento humano jamás acumulados en la historia y pueden emplear tal información para sus propios fines, sean los que sean, ya se trate de obtener

beneficios, proporcionar vigilancia, apoyar la investigación médica, facilitar la represión política o sobornar.

Ahora bien, si los datos son el petróleo de hoy en día, entonces al igual que los recursos naturales de siempre también deben salvaguardarse. No se dejan cien millones de barriles de petróleo desprotegidos y, por el contrario, en gran medida eso es justo lo que está sucediendo con la inmensa mayoría de los datos generados. La protección de nuestra información digital no se acerca ni por asomo a los niveles que debería tener. Los cien millones de barriles de petróleo están protegidos por guardias, vallas, armas, videocámaras y sensores instalados en el suelo y a todo lo largo de los oleoductos. Pero ¿qué pasa con los cien millones de tarjetas de crédito e informes sobre clientes que almacenan cadenas de comercios como Target? Tal como hemos visto, se guardan en bases de datos inherentemente inseguras y con escasa protección. Si se combinan esos inmensos tesoros de datos valiosos con la incapacidad de protegerlos, ¿qué crees que sucede? Nuestra capacidad para capturar y almacenar información aventaja sobremanera a nuestra habilidad para entenderla o entender sus implicaciones. Y por mucho que los costes empresariales de almacenar la información mundial se acerquen cada vez más cero, los costes sociales podrían ser mucho más elevados y plantear inmensas cargas en el futuro para nuestra sociedad y nuestro mundo.

En este sentido, la historia puede ser muy instructiva. Willie Sutton, el famoso atracador de bancos norteamericano, robó cerca de dos millones de dólares a lo largo de su carrera como delincuente, de varias décadas de duración, iniciada en los años veinte del siglo pasado. Tras ser apresado por el FBI, un periodista preguntó a Sutton: «Willie, ¿por qué robas bancos?». Su respuesta, repetida hasta la saciedad, fue: «Porque es donde está el dinero». Pese a que Sutton podía haber robado un dólar a dos millones de personas, escogió un planteamiento más lógico y eficiente en cuestión de tiempo y, en su lugar, decidió robar a los agregadores de divisas (bancos). Por el mismo motivo, no es ninguna sorpresa que los delincuentes vayan tras Target, Sony y otros agregadores de datos cuando la recompensa es tan elevada y los riesgos tan nimios, ¿no es cierto? En el mundo actual, es en los datos donde está el dinero.

Siguiendo el consejo de Gordon Moore y su ley epónima, yo también he determinado que hay un refrán que describe los riesgos asociados con las montañas crecientes de datos generados. Aquí te presento la ley Goodman:

> Cuantos más datos generas y guardas, más fácil se lo pones a las mafias.

Con el tiempo, tus datos personales caerán en manos de cárteles criminales, de la competencia e incluso de gobiernos foráneos[7]. Mientras que los datos masivos pueden ser el petróleo de hoy en día, nuestros datos personales son más bien plutonio para construir armas: peligrosos, duraderos e imposibles de recuperar una vez se filtran.

Incluso el gobierno federal está cayendo en la cuenta de que también podría ser víctima de este problema. Basta con observar la debacle de WikiLeaks en 2010 y los cientos de miles de mensajes diplomáticos clasificados que el soldado raso Chelsea (Bradley) Manning fue capaz de robar mientras trabajaba como analista para la inteligencia militar en Irak. Y al cabo de pocos años, el mundo conocería a Edward Snowden, que utilizó sus habilidades y su acceso como administrador de sistemas de la NSA para robar millones de archivos clasificados como confidenciales a Estados Unidos y sus aliados y los compartió con periodistas para su publicación en Internet. Algunos han afirmado que esta suerte de robo y revelación de información masiva constituye la «desobediencia civil de la era de la información». Pero si Manning y Snowden fueron capaces (supuestamente tras efectuar exhaustivas investigaciones de fondo) de acumular y robar volúmenes tan inmensos de datos comprometedores al gobierno federal, ¿qué podrían hacer si trabajaran para Target, Citibank o Apple? El aumento exponencial de datos empresariales significa que los secretos comerciales, los diseños de ingeniería, los conocimientos técnicos, las listas de consumidores, las tablas de salarios de los empleados, las estrategias de fijación de precios, los proveedores y cualquier información adicional almacenada en un dispositivo digital puede filtrarse. En la actualidad, cualquier empresa, al margen de su tamaño, puede tener a un Snowden en su seno, con notables implicaciones para la seguridad de sus datos, su privacidad y su viabilidad económica a largo plazo.

Un solo correo electrónico revelado de Facebook, Google o Apple puede brindar a los *hackers* acceso a años de tus mensajes de correo electrónico, citas en el calendario, mensajes instantáneos, fotografías, llamadas telefónicas, historial de compras en Amazon, cuentas bancarias y de acciones, y documentos en Dropbox o en Google Drive. Con todo, cabe destacar que las pérdidas de datos que imaginamos hoy empalidecerán frente a las posibilidades del mañana. En este mundo, nuestra capacidad de agregar toda la información generada tanto por seres humanos como por máquinas y almacenarla para la eternidad supera con creces nuestro entendimiento de los riesgos concomitantes.

¿Pésimos administradores de datos, víctimas de primera categoría o ambas cosas?

> Lo que yo hacía en mi juventud sería cientos de veces más fácil hoy. La tecnología engendra la delincuencia.
>
> FRANK W. ABAGNALE

Cuando Sony, Target y T. J. Maxx fueron víctimas de un ataque informático, ¿de

quién fue la culpa? ¿Fueron acaso estas empresas víctimas inocentes de ciberataques ingeniosamente inventivos perpetrados por sofisticados grupos transnacionales de la delincuencia organizada? ¿O sucedía por el contrario que eran profundamente laxas con sus precauciones en materia de seguridad y negligentes a la hora de implementar incluso las protecciones más básicas para los cientos de millones de cuentas que les habían confiado sus clientes? La respuesta es un punto intermedio entre ambos extremos. No son sólo los minoristas quienes están protegiendo de manera inadecuada los datos de sus clientes, sino también legiones de empresas noveles en Internet y los mastodontes de las redes sociales. Cuando facilitas de manera voluntaria tus datos a Facebook, Google y LinkedIn, entre otros, debes ser consciente no sólo de las numerosas ramificaciones para la privacidad que pueden tener tus actos, sino también de las posibles implicaciones delictivas. Estas empresas son víctimas de ataques informáticos rutinarios, y los datos que se hurtan son los tuyos. ¿Con qué frecuencia suceden estos ataques? Con mucha más de la que imaginarías nunca.

El departamento de seguridad de Facebook ha reconocido la alarmante noticia de que cada día se vulneran 600 000 cuentas. ¿Lo has entendido bien? No he dicho 600 000 cuentas al año ni al mes, sino al día. Eso representa una cuenta cada 140 milisegundos (se tardan 300 milisegundos en parpadear[8]). Estos datos pueden emplearse para suplantar identidades con fines delictivos, cometer fraude o evasión fiscal, estafar a las mutuas de salud y perpetrar otros delitos varios. Piensa en los tremendos volúmenes de datos personales que compartes en Facebook y ahora imagina lo que una mafia podría hacer con ellos. Nombre de soltera de tu madre: sí. Lugar de nacimiento: sí. Fecha de nacimiento: sí. Fotografías de tus hijos: sí.

Infiltrarse en tu cuenta de Facebook no es el objetivo final; es sólo el principio. Dado que el 75 por ciento de las personas utilizan la misma contraseña para diversos sitios web y el 30 por ciento usan la misma información de inicio de sesión para todas sus actividades en Internet, una vez queda al descubierto tu cuenta de Facebook, puede emplearse potencialmente para acceder a tu banco, tarjeta de crédito y cuentas de correo electrónico[9]. Además, cada vez más empresas externas te permiten utilizar tus credenciales de inicio de sesión en Facebook como pasaporte al resto del mundo digital. Si bien emplear la cuenta de Facebook para comprar, escuchar música y jugar a juegos es muy práctico, una vez esas credenciales de acceso únicas quedan comprometidas, sucede lo mismo con los demás servicios.

Muchas empresas de redes sociales han registrado filtraciones, incluidas LinkedIn (6,5 millones de cuentas), Snapchat (4,6 millones de nombres de usuario y números telefónicos), Google, Twitter y Yahoo[10]! Las mafias organizadas transnacionales son responsables de perpetrar el 85 por ciento de estas filtraciones y su objetivo no es otro que obtener la mayor cantidad de datos posible para poderlos vender al mejor postor en la ciberclandestinidad[11]. En ocasiones, las mafias organizadas ni siquiera necesitan piratear un sistema informático, porque se lo encuentran abierto de par en

par. De la misma manera que los depredadores de las llanuras del Serengueti no dudan en devorar a un animal que encuentran muerto en el camino, los piratas informáticos aprovechan felizmente cualquier tesoro de datos gratuitos que se les cruce por delante. Tal fue el caso, por poner un ejemplo, cuando la megaempresa de almacenamiento de datos en la nube Dropbox desactivó por accidente la necesidad de introducir la contraseña para cualquiera de las cuentas de toda su red en 2011[12]. Como consecuencia, cualquier persona podía leer cualquier archivo almacenado en la red de Dropbox.

Tal vez pienses que, si tus cuentas en las redes sociales o en Internet se piratearan de ese modo y sufrieras algún daño derivado, como la usurpación de tu identidad o el robo de decenas de miles de dólares de tu cuenta bancaria a causa de la negligencia de otra persona, tendrías el recurso de demandar a quienes han puesto en riesgo tu información. Por supuesto, no es así. Te has despedido de todos esos derechos al hacer clic en «He leído y acepto los términos y condiciones del servicio», una advertencia que hace que estas empresas resulten completamente ilesas cuando sufren un ataque de esta índole.

Facebook lo deja muy claro:

> Intentamos mantener Facebook en funcionamiento, sin errores y seguro, pero lo utilizas bajo tu propia responsabilidad. Proporcionamos Facebook tal cual, sin garantía alguna expresa o implícita. […] No garantizamos que Facebook sea siempre seguro o esté libre de errores. […] Nos dispensas a nosotros, nuestros directivos, empleados y agentes de cualquier demanda o daños, conocidos o desconocidos, derivados de o de algún modo relacionados con cualquier demanda que tengas interpuesta contra tales terceros.

Por cierto, no sólo la delincuencia organizada persigue los depósitos de datos masivos que has creado en Google, Yahoo! y Facebook, sino también los gobiernos, nacional y extranjeros. Por ejemplo, en enero de 2010, Google anunció públicamente que su red había sufrido un ataque masivo y culpó de éste al gobierno chino. Google informó de que las autoridades chinas tenían por objetivo acceder a las cuentas de Gmail de activistas en Estados Unidos, Asia y Europa que habían expuesto su preocupación por la protección de los derechos humanos en China. Otro objetivo de aquel incidente fueron secretos comerciales y el código fuente de Google, el mismísimo *software* con el que se ejecutan Google y sus productos.

Pese a que Google admitió el ataque, el alcance y la naturaleza exactos del robo se declararon secreto comercial. No obstante, posteriormente se reveló que unos piratas informáticos vinculados con el Ejército de Liberación Popular (ELP) chino habían hurtado el código fuente del sistema de gestión de contraseñas mundial de Google[13]. El robo del código fuente de Google podría haber provisto a los chinos de un acceso persistente a las contraseñas de millones de clientes de Google en todo el mundo y haber permitido al ELP permanecer oculto dentro de los sistemas de la empresa a largo plazo. ¿Has cambiado tu contraseña de Google desde 2010? Si no lo

has hecho, es posible que el ELP tenga una copia. Tanto si Internet y las empresas de redes sociales son pésimos administradores de nuestros datos, víctimas de primera categoría o un popurrí de ambas cosas, lo que importa es que cualquier dato que facilitemos a estos sitios web y estas empresas podría filtrarse y acabar en manos de delincuentes y terroristas, entre otros destinatarios finales.

Los intermediarios de datos también son pésimos administradores de tus datos

Uno de los problemas derivados de que los agentes de intermediarios de datos en la clandestinidad y apenas regulados acumulen inmensos volúmenes de información sobre nosotros es que estas empresas también pueden sufrir ataques informáticos. Cuando empresas como Acxiom almacenan billones de registros sobre cada uno de nosotros, esos registros se convierten en diana de la delincuencia organizada, porque, tal como nos recuerda Willie Sutton, es ahí donde está el dinero. Este robo de bases de datos a gran escala a los agentes intermediarios lleva produciéndose desde hace muchos años; de hecho, ya en el período de 2002 a 2003 se robaron más de 1600 millones de registros de clientes de Acxiom. De acuerdo con la documentación legal, el pirata informático responsable de aquel robo, Scott Levine, logró descargarse más de ocho gigabytes de archivos de Acxiom, cosa que se convirtió en uno de los mayores casos de intrusión relacionados con el robo de datos personales[14].

Más recientemente, en 2013, el agente intermediario de datos Experian vendió por error los datos personales de casi dos tercios de todos los estadounidenses a un grupo de delincuencia organizada de Vietnam[15]. Aquel fraude épico supuso que los números de la Seguridad Social de 200 millones de norteamericanos quedaron disponibles para ladrones de todo el mundo. Los conjuntos de datos obtenidos se conocían como «*fullz*» en la clandestinidad delictiva porque contienen el conjunto total de la información necesaria para que los delincuentes soliciten tarjetas de crédito y préstamos con los nombres de sus víctimas. Aquella infracción masiva de la seguridad tuvo lugar porque Experian no aplicó la diligencia debida con la organización pirata vietnamita, que había establecido una empresa fachada que se presentaba como un bufete de detectives privados estadounidense con el fin de adquirir los datos para sus objetivos delictivos. Lo has leído bien. Experian vendió 200 millones de archivos de datos de usuarios a un círculo de robo de identidades. Los datos acabaron poniéndose a la venta en docenas de sitios web de *hackers*, como SuperSet.info y FindGet.me, donde se vendían a la irrisoria cifra de entre dieciséis y veinticinco centavos por registro, y el único pago aceptado era mediante monedas online no rastreables, como Liberty Reserve y WebMoney. Experian tuvo noticia de

la infracción y de su complicidad en aquel asunto cuando fue contactada por los servicios secretos, que descubrieron la información a la venta en estos sitios web destinados a piratas informáticos[16].

Pero ¿por qué diantres iba una empresa supuestamente reputada a vender datos sin realizar las diligencias debidas? La respuesta, como siempre, es por dinero. Los agentes intermediarios de datos hacen dinero cuando venden datos, no cuando los protegen. En el transcurso de la investigación se desveló que delincuentes habían accedido a la base de datos vietnamita en al menos 3,1 millones de ocasiones antes de que ésta se desmantelara finalmente, pero, por supuesto, para entonces el daño ya era irreversible[17].

Dada la inmensa cantidad de datos disponibles sobre todos nosotros, las mafias han empezado a montar sus propias agencias de intermediación camufladas bajo empresas fachada y proporcionan datos obtenidos de manera ilícita a cualquier objetivo de interés particular. Un ejemplo de ello se vio cuando unos piratas informáticos rusos crearon un sitio web llamado Exposed.su para demostrar su potencia en materia de *hackeo* a otros colegas con tendencias delictivas a comprar… «acreedores de buena fe», si quieres llamarlo así. Aprovechando su capacidad de obtener datos sobre cualquiera, estos piratas informáticos albergaban de manera gratuita archivos de crédito sobre un gran número de figuras públicas, tanto pertenecientes a la política como a las fuerzas de seguridad y el mundo del entretenimiento.

Para obtener sus bienes ilícitos, los ladrones subvertían los sistemas de seguridad del sitio web de Equifax AnnualCreditReport.com y obtuvieron los informes crediticios completos de todos sus objetivos. Entre las víctimas del ataque había multitud de celebridades, incluidas entre ellas Ashton Kutcher, Kim Kardashian, Jay-Z, Bill Gates, Beyoncé, Robert De Niro, Lady Gaga y Sean Combs[18]. También se sustrajeron los informes crediticios de diversas figuras gubernamentales de perfil extremadamente alto, como la primera dama Michelle Obama, el vicepresidente estadounidense Joe Biden, el expresidente George Bush, el director del FBI Robert Mueller, el director de la CIA John Brennan y el Fiscal General, Eric Holder, además del jefe del Departamento de Policía de Los Ángeles, Charlie Beck.

Una vez los piratas de Exposed.su obtuvieron los informes crediticios completos de las personas listadas, los publicaron en Internet en formato PDF. Allí, expuestos a todo el mundo, quedaron los números de la Seguridad Social de las víctimas, sus fechas de nacimiento, todas las direcciones postales en las que habían residido, sus números telefónicos personales, las demandas legales presentadas contra ellas e información personal variopinta, como los cientos de miles de dólares que cargaban cada mes a sus tarjetas negras American *Express* o cuántos millones debían por sus hipotecas. Los informes crediticios de las personas afectadas se consultaron cerca de un millón de veces antes de que los sitios web acabaran desmantelándose[19].

Tal como he explicado en el capítulo anterior, los grandes agentes intermediarios

de datos elaboran listas muy segmentadas de individuos agrupados bajo epígrafes como «Caucásico, con estudios superiores, habitante del entorno rural, vive con su familia y le gusta cazar, pescar y ver las carreras de NASCAR». Y ahora parece que algunos de ellos empiezan a confeccionar listas para beneficio directo de los grupos de la delincuencia organizada, que pagarán los dólares que sean precisos por estas pistas delictivas. Los estafadores son una fuente lucrativa de ingresos para los agentes intermediarios de datos y, como tales, la industria de los datos elabora alegremente listas destinadas también a sus clientes delincuentes. Y aunque los agentes de datos rechazarían o renunciarían a cualquier responsabilidad por el uso que pudiera darse a dichas listas, los grupos de individuos con epígrafes como «pensionistas “ingenuos” que “quieren creer que su suerte puede cambiar”» no son más que una invitación a defraudar a ciudadanos ancianos los ahorros de toda su vida[20].

Para los agentes intermediarios de datos como ChoicePoint, Experian y Equifax, los incentivos económicos están gravemente desalineados desde la perspectiva de la seguridad y el riesgo público. Esto es particularmente cierto en la época de los datos masivos, cuando las mafias se encuentran manejándose en el sector de la gestión de conocimientos. Son una fuerza eficiente, efectiva y laboriosa en el mundo de los datos masivos y, cuantos más crean, más alegremente los consumen.

Los males de las redes sociales

Las redes sociales son un pasto ideal para la usurpación de identidad, pues lo único que precisan los ladrones de información para perseguirte está disponible en Internet de manera gratuita, ya sea tu fecha de nacimiento o el apellido de soltera de tu madre para acceder a tu cuenta de Facebook. Seguramente pensarás: «Los delincuentes no ven esa información. […] La tengo bloqueada en mis ajustes de privacidad». Ojalá los sistemas funcionaran tal como se anuncia. Hay múltiples motivos por los que cualquier información que publiques en Facebook se filtra. En primer lugar, como he indicado anteriormente, cuando Facebook actualiza sus términos y condiciones de servicio, suele *resetear* tus ajustes de privacidad a las opciones menos garantes de la privacidad existentes, con lo cual estos datos quedan a disposición de cualquiera, principalmente de sus anunciantes. En segundo lugar, con 600 000 cuentas en Facebook pirateadas a diario, es cuestión de tiempo que los delincuentes den con la tuya. Por último, puesto que «el dinero está ahora» en los datos sociales, los delincuentes han creado herramientas especializadas en la forma de virus específicos y troyanos para hacerse con tus cuentas en Facebook y otras redes sociales sin tu permiso.

Al menos el 40 por ciento de los usuarios de redes sociales han quedado expuestos a algún tipo de *software* malicioso, y más del 20 por ciento de nosotros

hemos visto como una tercera parte dejaba al descubierto o nos usurpaba la dirección de correo electrónico o una cuenta en las redes sociales[21]. Los malos engañan a los internautas para que hagan clic en enlaces de publicaciones y mensajes que supuestamente corresponden a amigos o colegas mediante una técnica conocida como «ingeniería social». Los delincuentes se aprovechan de la confianza que depositamos en aquellas personas que tenemos en nuestras redes sociales camuflándose electrónicamente como personas de confianza y engatusando invariablemente a los usuarios para que hagan clic en un enlace que acabará por infectarles el ordenador con un virus, un troyano o un gusano. Es más, las mafias organizadas reaccionan extremadamente rápido a las últimas noticias, que utilizan para embaucar a los usuarios inocentes para que cliquen en un enlace e infectar así sus ordenadores. Ya sea un terremoto en Haití, el arresto de Justin Bieber o el desnudo de Miley Cyrus, los titulares son demasiado suculentos como para no hacerles caso y los internautas acaban picando y clicando en los enlaces. Cuando el vuelo MH370 de Malaysia Airlines desapareció sobre el océano Índico, los estafadores estaban preparados para mostrar fotografías falsas del avión y supuestos vídeos en los que se veían los restos del «MH370 hallados en el mar, un impactante vídeo recién emitido por la CNN»[22]. Los mensajes se propagaron como un incendio forestal por las redes sociales hacia un público curioso y ansioso de respuestas, ajeno al hecho de que sus ordenadores acababan de ser infectados con un virus. A veces, la curiosidad mata al gato de verdad.

Uno de los programas de *software* malicioso más conocidos para las redes sociales es Koobface (una variación de «Facebook») e iba destinado a usuarios de Facebook de todo el mundo[23]. El dañino gusano concebido para las redes sociales se propagaba engañando a los usuarios para que hicieran clic en un enlace de Facebook con un titular demasiado seductor como para pasarlo por alto: «¡Madre mía! ¡Acabo de ver un vídeo en el que sales desnudo!». ¿Quién se resistiría a hacer clic en un mensaje así? Por desgracia, un clic motivado por la curiosidad podía desencadenar una ráfaga de *software* malicioso. Una vez infectado, el gusano de Koobface roba todas las credenciales de inicio de sesión que es capaz de encontrar en tu ordenador, incluidas las de las cuentas de Facebook, Skype, Yahoo! Messenger y Gmail. Koobface también puede forzar a tu ordenador a participar en ataques de denegación de servicio contra terceros y secuestrar tus resultados de búsquedas en la Red y clics para conducirte a sitios web peligrosos. Pese a que fue un grupo de piratas informáticos de San Petersburgo, Rusia, quien diseñó y propagó este *malware*, y a pesar de que los delincuentes responsables fueron identificados y sus nombres se revelaron públicamente, las autoridades rusas se han negado a extraditarlos para someterlos a un juicio por sus delitos[24].

Como es de suponer, las herramientas de ataque a las redes sociales se han racionalizado cada vez más en el presente y no hay que ser ningún genio de la piratería informática para sustraer información. Sin ir más lejos, Firesheep era un

sencillo módulo del navegador de Firefox que cualquiera podía descargar para colarse en la sesión de Facebook de otras personas conectadas a su misma red y secuestrar sus cuentas. De esta manera, si, por ejemplo, comprobabas tu cuenta de Facebook en un Starbucks del barrio donde compartías la red con otras veinticinco personas de la cafetería y una de ellas ejecutaba Firesheep, podía utilizar el módulo para conectarse en tu nombre en tu cuenta de Facebook[25]. Tan sencillo como eso. Una vez iniciada la sesión, el fisgón podía consultar toda tu información personal, modificar la configuración de tu cuenta y publicar lo que quisiera en tu muro o enviar mensajes a otros usuarios. Esta técnica se conoce como «secuestro de sesión» o *sidejacking* y es tan fácil de ejecutar que roza el ridículo.

Los delincuentes también atacan a usuarios de las redes sociales mediante aplicaciones de terceros y juegos online, ataques que les proporcionan acceso a tu cuenta bancaria y pueden dejarte en números rojos. Ésa fue la lección que aprendió Lisa Lockwood de Baltimore, Maryland, por las duras cuando la información que su hijo de diecisiete años había facilitado en una aplicación de juego de Facebook se volvió en contra de ambos. El juego ofreció al adolescente puntuación adicional a cambio de rellenar una aplicación que le solicitaba su número de la Seguridad Social. Sin pensárselo dos veces, y con la perspectiva de conseguir más puntos para «pasar de nivel» arremolinándosele en la cabeza, el adolescente rellenó la aplicación, ajeno a que ese número de la Seguridad Social sería utilizado por unos delincuentes para rellenar siete solicitudes de préstamo para coches distintas en su nombre en cuestión de días. La madre tuvo noticia del incidente cuando recibió una llamada telefónica de un concesionario de Subaru-Volkswagen local preguntándole acerca de la solicitud de crédito que había presentado su hijo[26].

Datos ilegítimos: el alma de la usurpación de identidad

La explosión de datos ha propiciado la aparición de un nuevo sector de mafias organizadas transnacionales, y la usurpación de identidad masiva es la principal consecuencia. De acuerdo con el Servicio de Investigación del Congreso de Estados Unidos, el fraude identitario costó a los estadounidenses cerca de 21 000 millones de dólares en 2012, y cada año más de 13,1 millones de norteamericanos son víctimas de fraudes derivados de la usurpación de la identidad[27]. Eso representa un estadounidense cada dos segundos[28]. Es más, el robo de esta información personal e identificable es como un portal para cometer toda una serie de delitos adicionales, como fraude financiero, fraude en aseguradoras, fraude fiscal, fraude al Estado del bienestar, inmigración ilegal e incluso financiación del terrorismo. El aumento exponencial de datos está derivando en un aumento exponencial de los delitos online.

Los niños son el grupo de víctimas de la usurpación de identidad que crece a un ritmo más alarmante. Son especialmente vulnerables porque carecen de los sistemas de advertencia que los adultos han desarrollado. Si alguien cargara de manera fraudulenta quinientos o mil dólares en tu tarjeta de crédito, seguramente te darías cuenta en el siguiente extracto que te enviaran, pero los niños no reciben extractos de tarjetas de crédito. Los ladrones que usurpan sus identidades pueden usarlas durante dieciocho años y sólo cuando estos jóvenes piden un crédito de verdad, como por ejemplo un crédito para estudiar en la universidad, descubren que sus posibilidades de obtenerlo han quedado aniquiladas por los usurpadores de información.

Sólo en Estados Unidos, 500 000 niños son víctimas de usurpación de identidad cada año[29]. De acuerdo con un estudio realizado entre 40 000 niños por el CyLab de la Carnegie Mellon University, los pequeños tienen cincuenta y una veces más probabilidades de ser víctimas de un robo de identidad que los adultos, una cifra asombrosa, sin lugar a dudas[30]. Desde bebés hasta adolescentes, son una diana fácil porque carecen de historial crediticio y, por consiguiente, son una tabula rasa para las mafias. Los padres no descubren los delitos ni la usurpación de sus identidades hasta muchos años más tarde, cuando, de súbito, deben hacer frente a los agresivos recaudadores de deudas que les solicitan que abonen los impagos de sus hijos. Dada la amplia medida en la que tanto niños como jóvenes viven ahora conectados a Internet y los métodos agresivos que los agentes intermediarios de datos y las grandes empresas emplean para perseguirlos, es lógico esperar que afrontarán amenazas importantes por parte de los usurpadores de identidad. Pero ¡ojalá estas penas financieras fueran su mayor problema! Como veremos, los datos que todos filtramos también pueden acarrear peligros físicos.

Acosadores, intimidadores y exparejas: el gran problema

Los volúmenes de datos acerca de ti que circulan por la Red no sólo resultan útiles para los ladrones de identidad, sino para otros muchos delincuentes, y son legión. Las nuevas tecnologías permiten perpetrar los viejos delitos cada vez con más facilidad, y los datos masivos permiten a los delincuentes tradicionales convertirte en una diana cada vez más precisa de sus fechorías. Gracias al estilo de vida que hemos adoptado y como parte del cual pasamos conectados a Internet las 24 horas del día, los siete días de la semana, todos somos localizables en todo momento, incluso por quienes no querríamos que nos localizaran. Lo más curioso de este fenómeno es que a menudo, mediante la información que proporcionamos de manera voluntaria o mediante las filtraciones de datos, somos nosotros mismos quienes facilitamos a los acosadores,

intimidadores y delincuentes que nos localicen.

Pongamos por caso el ciberacoso. Pese a que el acoso o *bullying* siempre ha sido un problema en las escuelas, Internet proporciona a los ciberacosadores acceso directo a sus víctimas, no sólo en el patio de la escuela, sino allá donde estén, en todo momento. Las amenazas llegan por medio de Internet, del correo electrónico, de las redes sociales, del teléfono móvil e incluso mediante aplicaciones de mensajería y juegos. De acuerdo con el Consejo Nacional para la Prevención del Delito de Estados Unidos, cerca de la mitad de los adolescentes son víctimas de ciberacoso[31]. Y parece que no hay salida para los jóvenes que afrontan un acoso constante: el 20 por ciento de los alumnos de secundaria admitieron «pensar seriamente en suicidarse» a causa del acoso online que padecían.

Los niños no son las únicas víctimas del ciberacoso, sino que este fenómeno afecta también a un número creciente de la población adulta. De hecho, el flujo de datos acerca de nosotros en expansión y nuestra presencia constante en línea han ayudado a transformar Internet en un terreno fértil para una nueva raza de delincuentes conocidos como «ciberacosadores». Estos delincuentes emplean Internet como «arma para hostigar, amenazar e intimidar a su presa». Los ciberacosadores actúan enviando correos electrónicos, mensajes de texto, publicaciones y tuits no deseados y difundiendo rumores en Internet acerca de la víctima. Aprovechando los datos que cada uno de nosotros filtramos a diario o disponibles a través de los agentes intermediarios, los ciberacosadores pueden obtener fácilmente información detallada acerca de sus víctimas, incluidas las direcciones de sus casas y sus trabajos y sus números telefónicos. A menudo, los ciberacosadores usan estos detalles para confrontar a sus víctimas en persona.

Facebook ha sido particularmente útil para los acosadores. Gracias a que cada uno de nosotros tiene cientos de amigos, a muchos de los cuales ni siquiera conocemos en persona, sería inteligente analizar con más cuidado quién envía realmente esas solicitudes de amistad. Christopher Dannevig utilizó Facebook para encontrar a su víctima, Nona Belomesoff, una mujer de dieciocho años de Sídney, Australia, y estudió meticulosamente su perfil antes de contactarla. Fueron las frecuentes publicaciones acerca de su amor por los animales que Belomesoff hacía en su página de Facebook lo que dio al acosador la idea de cómo convencerla para quedar con él. Aprovechando los datos publicados en la red social que la joven filtraba sin darse cuenta, Dannevig creó un perfil falso con el nombre de «James Green» y afirmaba trabajar en el Departamento de Recursos Humanos de un grupo de rescate de animales muy conocido a nivel local. El acosador de la mujer utilizó los detalles que ella misma había proporcionado para engatusarla. Tras crear el perfil falso, Dannevig contactó con Belomesoff e intercambiaron una serie de mensajes, hasta que finalmente consiguió «entablar amistad» con ella y granjearse su confianza. Poco después anunció que había una vacante en la ONG de rescate de animales en la que ella encajaría a la perfección. Belomesoff accedió a citarse con él para una entrevista

y el acosador se ofreció a llevarla en coche hasta el refugio animal ubicado en una zona aislada, justo a las afueras de Sídney. Emocionada ante la perspectiva de haber encontrado un empleo remunerado trabajando con animales, la joven accedió a ir en el coche con el hombre. Fue allí, en las afueras desiertas de Sídney, donde Dannevig la asesinó[32].

Pero las amenazas procedentes de extraños que utilizan nuestros datos para localizarnos y acosarnos en la vida real se quedan en mantillas en comparación con los peligros que afrontamos como resultado de la violencia doméstica y el riesgo en que nos ponen aquellas personas con quienes en el pasado compartimos una relación íntima. Facebook facilita seguir la pista a exnovios, exnovias o excónyuges con un grado normal, aunque insano, de curiosidad salaz. Las nuevas amistades, actualizaciones vitales, cambios en los estados de relación, viajes y planes de vacaciones son aspectos de gran interés para las exparejas. El fenómeno es tan común que la expresión «acoso en Facebook» ha entrado a formar parte del vocabulario corriente.

No obstante, en el caso de algunas personas, los datos que se filtran alimentan mucho más que la curiosidad por parte de sus exparejas. En las relaciones que han sufrido violencia doméstica en el mundo real, el 45 por ciento de las víctimas admitieron que sus maltratadores las persiguieron y atacaron también online, llegando a provocar que muchas de ellas padezcan síndrome de estrés postraumático. Los datos que damos en las redes sociales también aportan información relativa a nuestra localización y, dado que los maltratadores recorrerían el mundo para dar con sus víctimas, un inocente tuit, la actualización de un dato o la indicación de haber entrado en algún lugar puede ser, a efectos prácticos, tan peligroso como una bala. Por ejemplo, Paul Bristol voló de Trinidad a Inglaterra para matar a puñaladas a su exnovia tras ver publicada una fotografía de ella con su nuevo novio en Facebook[33].

Otro desafío en el mundo de los datos masivos es que la información que compartimos y pretendemos mantener en privado se filtra a otras personas. A menudo nos traicionan las mismas personas a quienes hemos confiado los detalles más íntimos de nuestras vidas, sobre todo mediante las fotografías compartidas. El llamado *sexting*, es decir: el compartir fotografías con contenido sexual explícito por SMS entre teléfonos móviles, es un fenómeno en alza, y un 67 por ciento de los estudiantes universitarios han admitido haberlo practicado[34]. Por desgracia, las fotografías compartidas de este modo no desaparecen por arte de magia y estos detritos de datos, como todos los demás, suelen volverse contra sus originadores de los modos más insospechados.

Sitios web como MyEx.com permiten a quienes han sido plantados compartir fotografías de sus examantes en un único sitio web. Hay más de setecientas páginas de fotografías de hombres y mujeres desnudos, con párrafos de quejas y acusaciones dirigidas hacia quienes aparecen en ellas: «¡No sabe follar!», «¡Me puso los cuernos con mi hermana!», «¡Pichacorta!». Hunter Moore, un joven de veinticuatro años, creó

IsAnyoneUp.com, un sitio web extraordinariamente popular que sirve de almacén de datos para cualquiera que quiera enviar fotografías de sus exparejas y enemigos desnudos y que recibe 250 000 visitas diarias[35]. El fenómeno ha devenido tan popular que incluso se lo ha bautizado con el nombre «porno vengativo». El sitio web de Moore está diseñado para listar junto a cada fotografía enlaces a las cuentas de Facebook o Twitter de la persona, e incluye su nombre completo y su lugar de nacimiento, información perfectamente indexada y recuperable en Google que aparecerá en cualquier búsqueda inocente que un tercero efectúe por el nombre de esa persona. Todas las fotografías de desnudos van acompañadas por una sección de comentarios que permiten al público, y al propio Moore, opinar sobre los protagonistas de las imágenes y ridiculizarlos[36].

Amenazas a menores en Internet

De acuerdo con el Pew Research Center, en la actualidad un 95 por ciento de los jóvenes estadounidenses tienen acceso a Internet y el 74 por ciento de los adolescentes entre doce y diecisiete años son usuarios de Internet móviles que a menudo acceden a la Red a través de sus teléfonos y tabletas[37]. Y un dato más importante aún: el 95 por ciento de los jóvenes entre diez y veintitrés años tienen al menos cuenta en una red social[38]. Gran parte de este acceso a Internet tiene lugar sin supervisión de sus padres, el 74 por ciento de los cuales aseguran que les desborda la tecnología moderna y no tienen ni el tiempo, ni la energía ni los conocimientos suficientes para supervisar las actividades online de sus hijos. Y es una lástima, porque, aunque el ciberacoso por parte de los propios compañeros es una de las principales fuentes de estrés para los jóvenes, afrontan peligros aún mayores en el mundo cada vez más conectado en el que vivimos.

Los depredadores de niños recurren a las tecnologías para canalizar todos sus esfuerzos hacia los niños con fines pederastas. Se trata de una práctica tan común, de hecho, que incluso hubo un programa en la televisión que hablaba de este fenómeno, el programa de la NBC *To Catch a Predator*. El desafío que afrontan los niños es que cuatro de cada cinco de ellos no saben discernir si su interlocutor en Internet es otro niño o un adulto que finge ser menor[39]. Su nueva amistad online, otra niña de ocho años del pueblo de al lado, podría ser perfectamente un hombre de cincuenta años residente a dos estados de distancia y dispuesto a cruzar las fronteras estatales para secuestrar a la pequeña.

Dado que los pedófilos tienen preferencias concretas con respecto a los niños a quienes persiguen (edad, sexo, color de pelo, altura, etc.), cualquier fotografía publicada en las redes sociales o en cualquier otro lugar de Internet puede utilizarse

como un catálogo de ventas o un mercado virtual para pederastas y pedófilos en busca de víctimas. Los pedófilos se esfuerzan por estar al corriente de los últimos juegos, servicios de mensajería y mundos virtuales de interés para los niños, y buscarán a sus víctimas en todos los foros online existentes, desplegando una variedad de herramientas que van desde las consolas Xbox hasta el iPad[40]. Y si crees que esa inquietante demanda de fotografías es limitada, has de saber que las fuerzas de seguridad han identificado al menos veintidós millones de imágenes y vídeos de este tipo sólo en Estados Unidos y algunos sitios web de pornografía infantil protegidos mediante contraseña albergan hasta treinta mil miembros de pago[41].

En la actualidad, el volumen de imágenes pedófilas aumenta, no sólo porque un adulto haya secuestrado a un menor y haya abusado de él o de ella, sino porque se ataca directamente a los niños mediante subterfugios e ingeniería social.

Tal fue el caso de Amanda Todd de la Columbia Británica, en Canadá, a quien, con doce años de edad, coaccionaron para que mostrara sus pechos en un sitio de chat de vídeo en directo, popular entre los adolescentes, conocido como blogTV[42]. La persona anónima que se lo pidió parecía agradable y piropeó y halagó a Amanda diciéndole que era muy guapa. En un momento de ingenuidad adolescente, Amanda le enseñó sus pechos, dando por supuesto que al otro lado había otro adolescente. Sin embargo, con el paso del tiempo cayó en la cuenta de que había topado con una fuerza mucho más siniestra. Un año después de «desnudarse», Amanda recibió un mensaje en Facebook de un hombre que, bajo un seudónimo, pedía a la niña que volviera a aparecer desnuda y realizara actos sexuales frente a la cámara para él. Si se negaba, la amenazaba con publicar el vídeo original de ella con los senos al aire. Para demostrarle que iba en serio, su acosador le indicó que sabía los nombres de sus amigos y familiares, su dirección y la escuela donde estudiaba y le aseguró que les mostraría el vídeo a todos[43]. La niña puso reparos y empezó el hostigamiento.

Su atormentador creó un perfil falso en Facebook con el nombre de Amanda y utilizó una imagen de sus pechos desnudos como fotografía de perfil. Luego empezó a enviar solicitudes de amistad a todos los amigos, familiares y profesores de Amanda que había descubierto en la cuenta auténtica de la niña. Amanda no tuvo noticia del incidente hasta que la policía, preocupada por sus repercusiones, llamó a la puerta de su casa a las cuatro de la madrugada del día de Nochebuena. Amanda estaba horrorizada. Al regresar a la escuela, la acosaron y hostigaron sin piedad. Aquella presión resultaba insoportable a la joven. Empezó a sufrir depresión y trastornos por ansiedad y pánico. Lloraba hasta dormirse cada noche y fue repudiada por todas sus amigas, que la acusaban de haber aparecido en aquel vídeo. Comía sola cada día a mediodía y empezó a mutilarse.

Para evitar el dolor y el ridículo, Amanda cambió de escuela y su familia se mudó a otra ciudad. Pero, por desgracia para ella, la persecución continuó. Su acosador llevaba un seguimiento de sus actividades online y creó una nueva página en

Facebook para mostrar a sus nuevos profesores y compañeros de clase aquel vídeo de ella sin la parte de arriba. En la nueva escuela, el acoso en el aula alcanzó tales dimensiones que un grupo de niñas se abalanzó sobre ella en el recreo, le propinaron puñetazos y acabaron echándola en una zanja de barro. Y para mayor ultraje aún, las niñas que la habían atacado colgaron un vídeo de su ataque en YouTube. Aquella tarde, Amanda regresó a casa y bebió lejía de una botella para poner fin a su dolor y a su sufrimiento. Una ambulancia la trasladó al hospital, donde le hicieron un lavado de estómago. Pese a que logró sobrevivir, el hostigamiento continuó. En su página en Facebook, otros estudiantes publicaron fotografías de contenedores de Clorox y la instaban a «esforzarse más la próxima vez». En respuesta, el 7 de septiembre de 2012, Todd publicó un vídeo de nueve minutos en YouTube detallando su lucha contra el acoso y las autolesiones[44]. En un vídeo muy emotivo, Amanda compartía sus experiencias con el acoso en la escuela mientras una música profundamente conmovedora sonaba de fondo. Poco después, el dolor se volvió demasiado insoportable y, a los quince años, Amanda se suicidó.

El vídeo de Amanda se hizo viral tras su muerte y fue visionado millones de veces. Algunos policías creían que Amanda podía haber sido víctima de «cappers», una inquietante tendencia como parte de la cual bandas de pedófilos online disfrutan convenciendo a niños para que se desnuden ante la cámara y los graban. Peor aún, los pedófilos utilizan luego esos vídeos para chantajear a los adolescentes para que realicen actos sexuales más explícitos tanto online como en persona[45]. La tragedia del asunto de Amanda Todd tiene diversas facetas. Una niña filtra inocentemente datos sobre ella misma online y es acosada tanto en las redes sociales como en el mundo real, hasta que decide poner fin a su vida. Pero, por muy trágico que pueda sonar, no se trata de un episodio aislado y la velocidad a la que esta tendencia acelera es preocupante. Los datos masivos comportan grandes riesgos, e incluso la información compartida de manera inocua por un adulto puede caer en manos de pedófilos.

En 2011, la policía de Melbourne, Australia, descubrió a diversos pederastas cuyas víctimas eran solitarias madres solteras con niñas pequeñas[46]. Para llegar hasta ellas, rastreaban sus perfiles online en busca de referencias a sus hijas. El objetivo de los pedófilos era abrirse camino en la casa, cosa que normalmente hacían con un nombre falso y un pretexto en un intento por iniciar una relación con la madre. Una vez los recibían en casa, el pedófilo utilizaba el tiempo que pasaba a solas para acosar a las hijas pequeñas de las madres solteras. Los delincuentes y depredadores juegan con reglas distintas y no tienen reparos en utilizar todos nuestros datos como cebo para un amplio abanico de consecuencias indeseadas.

Los que odian siempre odiarán

Tu perfil en las redes sociales también puede hacerte vulnerable a otro tipo de ataque, un delito motivado por la discriminación, como parte del cual fanáticos, racistas y homófobos ponen en su punto de mira a internautas en función de su raza, religión, credo, color, género u orientación sexual. Tales incidentes han acontecido ya en Facebook, Instagram, ICQ, Twitter y otras muchas redes sociales. Facebook fue acusado de albergar un discurso del odio tan violento que la CNN publicó un reportaje titulado «Facebook/Hatebook?»[*] para documentar este fenómeno.

Los datos en Internet permiten a los criminales localizar a víctimas basándose en sus preferencias. En un caso, un asaltante de Texas atacó a un hombre homosexual a quien había conocido en la plataforma de redes sociales MeetMe.com. Tras concertar una cita con la víctima, el atacante lo secuestró, lo golpeó hasta dejarlo inconsciente, le ató las muñecas y lo metió en el maletero de su coche antes de arrojarlo a la cuneta[47]. Brice Johnson de Fort Worth fue acusado del ataque y, al ser arrestado, alegó que sólo quería darle una lección a aquel homosexual, pero admitió que «la broma se le había ido de las manos».

Mas por espantoso que pueda parecer este incidente en Texas, el volumen de delitos por motivos de discriminación en Estados Unidos empalidece en comparación con el de Rusia, donde se acreditan miles de ataques a un nuevo movimiento de jóvenes neonazis en el país. En un documental de una hora de duración producido para el Channel 4 del Reino Unido, el equipo de periodistas documentó más de 1500 secuestros en los que bandas de justicieros cazaban a chicos jóvenes en las calles y en Internet[48]. Las víctimas, en su mayoría adolescentes, eran secuestradas, golpeadas y aterrorizadas durante los secuestros, que a menudo, además, se filmaban sin reparos. Los atacantes no temen que la policía del país, cómplice, los represalie, cosa que los ha espoleado a publicar los vídeos de sus brutales palizas tanto en Facebook como en Instagram, en un esfuerzo por humillar aún más a las víctimas[49]. Pese a los volúmenes de pruebas documentales publicadas en Internet en centenares de casos, no se ha producido ningún arresto ni juicio, ni siquiera cuando las víctimas fueron asesinadas o quedaron discapacitadas para siempre…, una extraña incongruencia dada la destreza de la policía rusa para monitorizar sistemáticamente toda la actividad en Internet que tiene lugar en el país en las distintas redes sociales.

Robos en domicilio 2.0

¿Alguna vez has publicado en Facebook que te ibas de vacaciones? Un porcentaje asombrosamente alto de personas no tienen reparos en hablar acerca de sus futuros planes de viaje online, y mencionan, por ejemplo, las ganas locas que tienen de visitar Disney World o de disfrutar de una escapada de fin de semana en la playa. Sin

embargo, de lo que no se dan cuenta es de que los delincuentes son perfectamente capaces de recuperar esos datos en Internet y utilizarlos para sus propios objetivos (recuerda la ley de Goodman: *cuantos más datos generas y guardas, más fácil se lo pones a las mafias*).

En el pasado, si un caco quería colarse en una vivienda, normalmente buscaba signos que delataran que los inquilinos estaban de vacaciones, como, por ejemplo, una pila de diarios delante de la casa o una luz en el porche que permanecía encendida toda la noche. Pero incluso los cacos han modernizado sus herramientas y cada vez recurren más a las tecnologías para localizar sus objetivos y los hogares donde robar. Bienvenido al mundo de los robos en domicilio 2.0. Estos delincuentes revisan cada vez más tus publicaciones en Facebook, Google+ y Twitter y utilizan los datos sobre ti que se filtran para generarse nuevas «oportunidades de negocio», de la misma manera que lo haría cualquier otro vendedor o prospector de negocio. Para recalcar esta amenaza, un grupo de programadores informáticos holandés preocupado por el exceso de datos que compartimos creó un sitio web llamado PleaseRobMe.com[50]. Allí agregaban datos de localización extraídos de los tuits y *check-ins* con Foursquare de las personas y creaban una base de datos con la información recopilada, que podía consultar cualquiera. El resultado: los posibles ladrones podían comprobar por código postal quién estaba de vacaciones y durante cuánto tiempo y, por consiguiente, saber con facilidad si podían robar su domicilio o no. Selección de objetivos con un simple clic del ratón.

No se trata de una amenaza puramente hipotética: los cacos del mundo real hacen un seguimiento de los datos sociales. Un ejemplo salió a la luz en 2010, cuando un grupo de delincuentes de Nashua, New Hampshire, se conectaron a Facebook para determinar si sus víctimas estaban en casa o no. La policía de Nashua descubrió que aquel grupo de delincuentes habían comprobado las actualizaciones de Facebook de sus víctimas antes de perpetrar los más de cincuenta allanamientos de morada y robar artículos por un valor cercano a 200 000 dólares durante su parranda delictiva[51]. No estamos hablando de los cacos que robaron a tu abuelo, sino de delincuentes que adoptan rápidamente las tecnologías que los ayudan a cometer nuevos delitos. De acuerdo con un estudio realizado en 2011 entre los ladrones de domicilios convictos en el Reino Unido, el 78 por ciento de ellos admitió monitorizar Facebook, Twitter y Foursquare antes de seleccionar una vivienda específica para robar. También confesaron usar herramientas como Street View de Google para revisar el aspecto externo de la vivienda de antemano y determinar posibles vías de huida del escenario del crimen[52]. Los resultados destacan los métodos a los que recurren los delincuentes para utilizar los datos que filtramos en nuestro perjuicio.

Otro modo que los cacos tienen de ponerte en su diana es mediante los datos de localización incrustados a los archivos que publicas en Internet. Tal como he señalado previamente, los llamados metadatos se implantan de manera tácita y se ocultan en las fotografías, vídeos y actualizaciones de estado que compartes a través de tus

dispositivos móviles y revelan la fecha y la hora en las que se tomó la fotografía, el número de serie del teléfono o de la cámara y, lo que es más importante, la longitud y la latitud (coordenadas del GPS) del lugar donde se tomó la imagen. Los metadatos que contienen esta información, pese a no ser inmediatamente evidentes a la hora de visionar un vídeo o ver una fotografía, son perfectamente accesibles para cualquiera que sepa cómo descargar un módulo *plug-in* de navegador para acceder a ellos. Con cualquiera de los cientos de herramientas gratuitas que existen, súbitamente tus fotografías cobran vida y aparecen como por arte de magia en un mapa de Google que permite a cualquiera ampliar la imagen y ver la ubicación precisa en la que se tomó la imagen. Tal es el milagro de la ciberlocalización o *cibercasing*: utilizar datos de geolocalización ocultos para planificar delitos.

Esos mismos datos se incorporan a millones de fotografías publicadas en sitios web de venta y subasta como Craigslist e eBay. Por ejemplo, una fotografía de un anillo de diamantes o un iPad aparecidos en Craigslist podrían llevar incrustada la ubicación exacta de tu hogar, donde se tomó la imagen. Esta información permite a los ladrones versados en tecnologías emplear Craigslist como un sencillo catálogo comercial de artículos que no tardarán en ser robados[53].

Cuando Keri McMullen y Kurt Pendleton de New Albany, Indiana, decidieron vender su televisor de plasma y sistema de música estéreo, publicaron fotografías de ambos en Internet. Al cabo de pocos días, la pareja mencionó en Facebook que asistiría a un concierto en la cercana Louisville aquel sábado por la noche[54]. Ésa fue toda la información que los ladrones necesitaron para robar un hogar con los artículos electrónicos que les interesaban. Los ladrones sabían que disponían de tiempo porque la pareja estaría varias horas en el concierto. Al final, les robaron el televisor de pantalla plana, dos ordenadores portátiles, un equipo estéreo con todos sus componentes y una cámara digital de 35 mm de gama alta. Y éste es sólo uno de los usos que los delincuentes dan al comercio electrónico: catalogar tu hogar desde dentro con los datos que tú mismo filtras.

Estafas y asesinatos de objetivo conocido

Otro modo como los delincuentes aprovechan nuestras publicaciones online sobre las vacaciones y nuestras actualizaciones de estado acerca de viajes es timando a tus abuelos. Como lo oyes: los delincuentes monitorizan tus redes sociales y ven cómo publicas fotografías de tus vacaciones en tiempo real. Una vez lo has hecho, los artistas del timo exploran tus redes sociales en busca de parientes ancianos, normalmente tus abuelos, a quienes notifican que has tenido «un desgraciado accidente». El timo consiste en decirles algo así: «Hola, ¿hablo con la abuela de Peter? Sí, tengo malas noticias. Su nieto Peter se ha visto involucrado en un terrible

accidente en Barbados. El hospital no acepta el seguro estadounidense y se niega a tratarlo hasta que hayamos abonado los 10 000 dólares que cuesta el quirófano. Si no lo ayudan, es posible que no viva para contarlo». ¿Cómo consiguen los timadores salirse con la suya? Porque les ayudamos, aunque sea de manera inconsciente, mediante la información que compartimos en este nuevo mundo de los datos masivos en que vivimos. Facebook le explica al mundo (en el cual viven también las mafias organizadas) quiénes son nuestros padres y cómo dar con la ancianita tía Margaret para presionarla: «No pinta bien […] Peter está en coma… ¡Por favor, envíen el dinero inmediatamente!». Centenares de personas han sido víctimas de este timo, que ha visto cómo se transferían millones de dólares vía Western Union y MoneyGram[55].

Y mientras que los timadores en Internet que monitorizan tus cuentas en las redes sociales pueden costarte varios miles de dólares, cuando los narcotraficantes deciden seguirte en Twitter puede costarte la vida. Los cárteles de la droga aplican una amplia variedad de sofisticados programas de contraespionaje para recopilar datos de las plataformas de redes sociales, blogs y líneas de colaboración ciudadana como medio de conocer sus amenazas potenciales.

Los comentarios hechos en Internet que los cárteles perciben como desfavorables para ellos se cortan por lo sano. En septiembre de 2011, al otro lado de la frontera de Texas en Nuevo Laredo, México, los habitantes que iban de camino al trabajo a pie de buena mañana tropezaron con dos cadáveres atados de brazos y piernas colgados de un paso elevado peatonal[56]. Las víctimas, un hombre y una mujer veinteañeros, habían sido sometidos a todo tipo de torturas y a la mujer la habían destripado. Por encima de los cuerpos colgados, un gran rótulo advertía siniestramente: «Esto es lo que les pasará a todos los chivatos de Internet… Ten cuidado: te estamos vigilando. Firmado: Z», una referencia a los Zetas, uno de los cárteles del narcotráfico más importantes y violentos de México. Estos cárteles tratan con una destreza parecida sus campañas en las redes sociales, donde cargan fotografías y vídeos de sí mismos en Facebook y Twitter en plena decapitación de sus víctimas con sierras mecánicas y machetes[57].

Entre tanto, los terroristas no sólo utilizan las redes sociales con fines operativos, tal como hemos visto que hicieron en Bombay, sino que también tuitean en tiempo real para influir en la opinión pública y atemorizar más a sus objetivos. Durante el atentado en septiembre de 2013 al centro comercial de Westgate en Nairobi, Kenia, los miembros del grupo Al-Shabab que perpetraron el ataque tuitearon en directo su matanza desde el interior del centro comercial. Los terroristas con sede en Somalia asesinaron a sesenta y tres civiles inocentes y ocasionaron cerca de doscientos heridos. Incluso publicaron fotografías en Twitpic de la matanza en el interior del Westgate y acusaron al gobierno keniata de destruir el centro comercial, con el *hashtag* #Westgate.

Implicaciones para el contraespionaje de los datos gubernamentales filtrados

Las mafias y las organizaciones de narcotraficantes utilizan las redes sociales para espiar a los agentes gubernamentales y a las fuerzas de seguridad. Por ejemplo, cuando en 2010 dos ayudantes del *sheriff* del condado de Maricopa, Arizona, obligaron a detenerse a un vehículo por conducción bajo la influencia de estupefacientes, al registrarlo descubrieron varios discos CD con datos, incluido uno con los nombres, fotografías y perfiles de Facebook de cerca de treinta agentes de policía y agentes secretos[58]. A los agentes no estatales y a los grupos *hacktivistas* como Anonymous y LulzSec también les interesan los datos que los funcionarios del gobierno filtran en las redes sociales.

En un incidente ocurrido en 2012, el grupo *hacktivista* LulzSec demostró su capacidad de robar datos incluso al FBI. Dado que la organización *hacktivista* había empezado a pinchar las direcciones de correo electrónico personales de varios agentes de policía, sobre todo de los que trabajaban en la lucha contra la ciberdelincuencia, podían interceptar cualquier notificación por correo electrónico de una teleconferencia entre el FBI, Scotland Yard y otros organismos policiales del resto del mundo. ¿El asunto de la llamada? Discutir «las investigaciones en curso relacionadas con Anonymous, LulzSec, Antisec y otros grupos disidentes»[59]. Una vez en posesión de la dirección de correo electrónico, los *hacktivistas* no tenían más que utilizar la información de establecimiento de llamada y el código de acceso para participar tácitamente en la comunicación. Mientras los principales cuerpos de seguridad del mundo discutían el caso contra Anonymous y LulzSec, había *hackers* conectados a la línea escuchando a la policía que, sin saberlo, los ponía al día de los progresos de la investigación. LulzSec, incluso grabó la llamada, que luego colgó en YouTube, para bochorno de las autoridades policiales implicadas y socavamiento de la investigación[60].

Entonces ¿es mejor no tener ningún perfil en línea?

No necesariamente. Dados todos los riesgos derivados de publicar datos online en redes sociales, podría parecer que no participar en Facebook o LinkedIn serían la solución obvia. Sin embargo, boicotear las redes sociales también comporta sus propios desafíos. Si no tienes y controlas tu propia imagen personal en Internet, a cualquier delincuente le resultará sumamente sencillo agregar los datos públicos que se conocen de ti y usarlos para perpetrar toda suerte de actividades delictivas, desde usurpación de identidad hasta espionaje. De hecho, abundan los ejemplos en los que

así ha sucedido, sobre todo en personas con gran notoriedad. A título de ejemplo, a finales de 2010, un grupo de la delincuencia organizada se apoderó de la identidad del secretario general de la Interpol, Ron Noble, y creó una página web en Facebook en su nombre[61]. Los delincuentes tomaron su fotografía oficial del propio sitio web de la Interpol y extrajeron los datos de su biografía oficial para componer un perfil falso en la red social. El grupo de delincuencia organizada empezó a recabar entre sus amistades a otras autoridades importantes de los cuerpos de seguridad de todo el mundo haciéndose pasar por Noble y plantearon preguntas operativas sobre sí mismos mediante los servicios de la red social. En concreto, los delincuentes que fingían ser Noble intentaban recopilar información con respecto a la Operación Infrarrojo, una operación mundial encubierta de la Interpol cuyo objetivo era localizar y arrestar a fugitivos internacionales de máxima prioridad. Se desconoce cuántos sucumbieron a aquel ardid y qué cantidad de datos se compartieron, pero docenas de agentes de policía de alto rango en todo el mundo aceptaron las supuestas solicitudes de amistad.

El espía al que le gusté

El espionaje industrial también ha hallado un poderoso aliado en las redes sociales[62]. En el segundo capítulo de este libro hemos visto cómo la empresa de turbinas eólicas de Massachusetts AMSC perdió casi mil millones de dólares en su valoración después de que le hurtaran el código fuente informático mediante una operación de espionaje china[63]. Sin embargo, lo que no hemos explicado es cómo se perpetró el ataque.

Cuando los funcionarios chinos decidieron robar el código fuente en nombre de Sinovel, una empresa de propiedad estatal a la cual AMSC suministraba turbinas eólicas, una simple comprobación en LinkedIn habría proporcionado a sus agentes acceso al listado de los empleados de la empresa de Massachusetts. Una vez los chinos hubieron completado la revisión de todos los empleados y los puestos que ocupaban, se generó una lista destacando aquellos objetivos que probablemente tenían un mayor acceso al valiosísimo código fuerte de AMSC. Una de las personas identificadas fue un ingeniero serbio que trabajaba para la oficina de AMSC en Austria llamado Dejan Karabasevic.

Los chinos comenzaron a monitorizar a Karabasevic en una serie de redes sociales, incluidas LinkedIn, Facebook y Twitter. Supieron que estaba atravesando un divorcio amargo y que recientemente había sido degradado en su puesto de trabajo, justo el tipo de vulnerabilidades que cualquier agencia de espionaje actual busca a la hora de seleccionar a posibles reclutas. A través de sus diversas publicaciones, los

chinos fueron capaces de recrear el «patrón de vida» de Karabasevic y localizar en un mapa su gimnasio, sus restaurantes, cafeterías y bares preferidos, su hogar y su oficina, la duración del trayecto entre ambos puntos y sus rutinas diarias. También averiguaron que sentía inclinación por las mujeres asiáticas. Armados con toda esta información, iniciaron su proceso de captación[64].

Unos encargados de una empresa china se aproximaron a Karabasevic y le ofrecieron una oportunidad de trabajar con ellos «como asesor». Al final, lograron convencer a Karabasevic para que les proporcionara el código fuente (la fórmula secreta) que permitió a Sinovel construir sus propias turbinas eólicas sin AMSC. Y lo más importante para Karabasevic, sus supuestos empleadores chinos le instalaron una oficina en Pekín para él y le prometieron «todo el contacto humano que quisiera […] especialmente con sus colegas mujeres». Después del robo salieron a la luz centenares de conversaciones por chat en Skype y mensajes de correo electrónico entre Karabasevic y sus empleadores chinos. En una nota, Karabasevic escribió: «Lo único que buscan las mujeres es dinero. Yo necesito mujeres. Y Sinovel me necesita»[65]. Para aliviar sus tribulaciones económicas, satisfacer sus necesidades de compañía y apuntalar el balance de Sinovel, los chinos ofrecieron a Karabasevic 1,7 millones de dólares a cambio del código fuente. El trato económico es fascinante a la par que instructivo: Karabasevic recibe 1,7 millones de dólares; AMSC pierde mil millones de dólares en valoración y propiedad intelectual, de los que Sinovel se apodera vendiendo, supuestamente, productos de AMSC pirateados en todo el mundo. Una gran rentabilidad de la inversión para Sinovel y para aquéllos sin remordimientos por las implicaciones morales de un pacto de estas características.

Como debería ser evidente a estas alturas, son múltiples los riesgos de la marea de datos que nos arrastra, y que no deja de aumentar exponencialmente. No sólo nos enfrentamos a una arremetida de minería de datos por parte de empresas de Internet, comerciantes y agentes intermediarios externos, sino que también los delincuentes, terroristas y gobiernos corruptos nos tienen sometidos a ataques y vigilancia constante, y acumulan y agregan esos datos sin cese. Con todo, estas estelas de detritos de datos se multiplican exponencialmente gracias a los ordenadores que llevamos siempre encima: los teléfonos móviles.

Capítulo 7

T. I. Al teléfono

> Los teléfonos móviles son uno de los dispositivos más inseguros que hayan existido nunca, por lo cual resultan muy fáciles de rastrear y de pinchar.
>
> EVGENY MOROZOV

El 21 de marzo de 2002, Milly Dowler, una muchacha de trece años de Surrey, Inglaterra, telefoneó a su padre para decirle que no tardaría en llegar a casa[1]. Horas más tarde, la adolescente aún no había llegado y no respondía a las llamadas a su teléfono móvil. La tarde del día siguiente se organizó una búsqueda masiva por la zona y los telediarios nacionales se hicieron eco de la desaparición de Milly[2].

Como parte de su investigación, la policía de Surrey accedió al buzón de voz del móvil de la joven desaparecida en búsqueda de pistas[3]. Las comprobaciones con su teleoperadora de telefonía móvil revelaron que cinco días después de su desaparición, alguien había accedido al buzón de voz y alguien desconocido había escuchado un nuevo mensaje que había llegado aquel día. Aquel descubrimiento alimentó las esperanzas de los Dowler de encontrar a su hija con vida. A medida que las semanas avanzaban pesadamente, continuaron escuchándose y borrándose mensajes del buzón de voz de Milly, lo cual llevó a los investigadores a plantearse si la muchacha no se habría escapado de casa.

Por desgracia para los Dowler, Milly no se había fugado, sino que la habían secuestrado: su cadáver fue hallado a cuarenta kilómetros de donde había sido vista con vida por última vez seis meses antes[4]. En un instante, el caso de Milly dejó de considerarse el de una persona desaparecida y dio paso a una investigación a gran escala por homicidio. Pero un hecho continuaba confundiendo a la policía: ¿quién había accedido repetidamente al móvil de la joven tiempo después de que desapareciera y se la diera por muerta? ¿Sería el asesino? ¿Un novio celoso? ¿Sus padres tal vez? Durante cerca de una década, aquella pregunta persistente permaneció sin respuesta, hasta junio de 2011, cuando finalmente se resolvió el misterio. Nadie habría imaginado quién era el culpable.

En un extenso artículo publicado por el diario *The Guardian*, se reveló que el teléfono de Milly figuraba entre los pinchados por el diario de Rupert Murdoch *News of the World* como parte de un escándalo que la prensa británica bautizó con el nombre de Hackgate. Ni el asesino, ni los padres ni el novio de Milly habían pinchado su teléfono, sino alguien con ganas de presentar una exclusiva en las páginas de su tabloide. Ahora bien, la pobre Milly y los Dowler no fueron las únicas

víctimas del Hackgate, sino que las acompañaron en aquel asunto numerosas celebridades, políticos e incluso miembros de la familia real británica, lo cual podría tener sentido dada su notoriedad. Pero lo cierto es que con el tiempo se descubrió que los periodistas e investigadores privados que *News of the World* contrató habían extendido sus operaciones de robo de datos móviles mucho más allá de las figuras públicas de perfil alto. En un gesto deplorable, también habían pinchado los teléfonos de los parientes de los soldados británicos asesinados en Irak y Afganistán y de las víctimas de los trágicos atentados con bomba del 7-J en Londres[5]. Los abominables detalles del caso causaron un revuelo público internacional y el cierre del diario de Murdoch *News of the World* tras 168 años de publicación ininterrumpida. Docenas de empleados y trabajadores independientes para el diario fueron arrestados, incluido el investigador privado contratado para obtener detalles de la desaparición de la niña[6].

Por supuesto, a aquellos dos padres en duelo poco reconfortaron las sanciones y los arrestos de los implicados[7]. A los Dowler les parecía tan enrevesado que un diario hubiera quebrantado la seguridad del teléfono de Milly que les resultaba inconcebible. ¿Había entorpecido la investigación del paradero de su hija de trece años desaparecida el hecho de que hubieran pinchado su móvil de manera ilegítima? ¿Qué recursos policiales se desperdiciaron intentando llegar al final de lo que parecía una pista importante que posiblemente hubiera dejado atrás el sospechoso del asesinato de Milly, un tiempo precioso que podría haber impedido su trágica y prematura muerte? Nunca lo sabremos, ni tampoco lo sabrán los Dowler, que tendrán que vivir con la tragedia y con esa angustiante pregunta cada día del resto de sus vidas.

Mas, pese a que tales actos son en efecto deplorables, lo más triste es que son muy fáciles de perpetrar. La seguridad de nuestros teléfonos móviles (ese dispositivo al que a la mayoría de los ciudadanos tenemos tanto apego) es una farsa que tanto las mafias como los acosadores, terroristas e incluso los periodistas sin moral ni un ápice de decencia aprovechan en beneficio propio.

La inseguridad del sistema operativo de los teléfonos móviles

Los teléfonos móviles se están convirtiendo en nuestros ordenadores preferidos. Estos «soplones que llevamos en el bolsillo» actúan de faros constantes que señalizan nuestras actividades y nuestra ubicación. De la misma manera que los teléfonos móviles son un tesoro de datos para los anunciantes, también lo son para los delincuentes. Aún peor, los teléfonos móviles son los dispositivos menos seguros de todos. El *software* que emplean es célebre por la facilidad con la que puede

vulnerarse, no se tiene constancia de los riesgos y los sistemas de protección del dispositivo son inmaduros y están completamente infradesarrollados. En consecuencia, los *smartphones* figuran entre los dispositivos más fáciles de piratear. Si bien los cuerpos policiales y las fuerzas de seguridad llevan años pinchando teléfonos, ahora esas mismas técnicas están perfectamente disponibles para empresas delictivas y *hackers* de poca monta.

En la actualidad, existen virus y troyanos diseñados específicamente para brindar a los atacantes acceso al micrófono de tu teléfono móvil y grabar los sonidos del entorno, incluso aunque no se esté efectuando una llamada. Todo lo que hagas y todo lo que almacenes en tu móvil (todo tu historial de mensajes de texto, tu agenda, fotografías, registros de llamadas, contraseñas de redes sociales e información de cuentas) puede ser interceptado, pirateado y transmitido a organizaciones delictivas para su explotación futura.

Los delincuentes pueden utilizar el *software* malicioso para teléfonos móviles para realizar un seguimiento de tu localización en tiempo real, con la ayuda práctica de un mapa de Google. Incluso es posible activar la videocámara de tu teléfono inteligente para grabarte (sin que se encienda ninguna luz de advertencia). Hay tantos vídeos de YouTube, sitios web con instrucciones y programas informáticos delictivos prefabricados a la venta que incluso los más novatos pueden piratear un teléfono móvil. De hecho, suele ser tan fácil como enviar un SMS infectado a tu objetivo.

Es legítimo preguntarse cómo es posible que los teléfonos móviles sean tan fáciles de vulnerar. La respuesta es que el problema radica en el sistema operativo. Los sistemas operativos de los teléfonos móviles son más nuevos que sus homólogos de sobremesa de toda la vida y mucho menos seguros. Los delincuentes son plenamente conscientes de que el mundo de los datos masivos cada vez funciona más en dispositivos móviles y ahí es donde están concentrando todos sus esfuerzos para garantizarse el mejor retorno por sus inversiones en *software* malicioso. Los móviles son la plataforma predilecta. Son dispositivos personales y siempre los llevamos con nosotros, y los delincuentes se adaptan e innovan con celeridad.

En 2014, McAfee había identificado cerca de cuatro millones distintos de pequeños programas de *malware* para teléfonos móviles, un aumento del 614 por ciento con respecto al año previo[8]. Es más, de acuerdo con un estudio realizado por Cisco (y ampliamente publicitado por el vicepresidente sénior de *marketing* internacional de Apple, Phil Schiller), el 99 por ciento de todo el *malware* móvil va destinado contra el sistema operativo móvil de Google: Android[9]. Tales hallazgos son hondamente inquietantes, sobre todo habida cuenta que el 85 por ciento de los teléfonos inteligentes distribuidos en todo el mundo a mediados de 2014 eran Android y está previsto que para 2017 se hayan distribuido mil millones de dispositivos móviles Android adicionales[10]. Sin lugar a dudas, la naturaleza de código abierto del sistema operativo Android es uno de los principales activos de la plataforma para incrementar sus ventas, pero tal abertura y la disponibilidad de

personalizar el *software* gratuito de acuerdo con las preferencias personales pone en jaque un activo importante: la seguridad. La mayoría de los fabricantes de dispositivos y operadoras telefónicas implementan el *software* sin demasiado esmero.

Pero ¿por qué es tan fácil sustraer datos de los dispositivos Android? Simple y llanamente, por la falta de actualizaciones y corrección de errores del sistema operativo para teléfonos móviles. Son las operadoras telefónicas las que distribuyen a los usuarios de Android las nuevas versiones del sistema a modo de actualizaciones obligatorias. Además, las operadoras y los fabricantes de dispositivos deben modificar cada nueva instalación de Android y personalizarla para que funcione con cada modelo de teléfono, un proceso costoso que consume mucho tiempo y hace que haya menos actualizaciones por dispositivo en el mundo Android. Peor aún, de acuerdo con varios estudios, son este proceso de personalización y el *software* poco seguro que añaden las empresas de telefonía móvil y los fabricantes de dispositivos lo que degenera en el 60 por ciento de las amenazas de seguridad del ecosistema Android[11]. Todas esas aplicaciones e interfaces molestas que incorpora el teléfono reciben el nombre de *bloatware*, «*software* inflado» o «*software* innecesario», porque ocupan espacio del dispositivo, poseen un valor dudoso y únicamente funcionan como trucos comerciales para el fabricante del dispositivo o la operadora de Wi-Fi. No sólo son fastidiosas, sino que su implementación realizada sin demasiado análisis propicia la mayoría de las amenazas a la seguridad que afectan a los dispositivos Android.

En comparación, Apple controla íntegramente los ecosistemas de su *hardware* y *software*. Gracias a ello, puede garantizar que el *software* de su sistema operativo para iPhone (iOS) funcione mucho mejor y a las operadoras se les prohíbe alterar fundamentalmente el sistema operativo subyacente con su *software* innecesario. De ahí que la comparación entre Android e iOS sea reveladora: cinco meses después de su estreno en 2013, el 82 por ciento de los 800 millones de dispositivos Apple utilizaban el sistema 7, la versión más actualizada del iOS. En cambio, sólo un 4 por ciento de los usuarios de Android ejecutaban la versión más nueva del sistema operativo para móviles de Google, lanzado al mercado aquel mismo año[12]. Lo más frustrante con relación a estas cifras es que, si todos los usuarios de Android pudieran actualizar sus sistemas a la última versión de manera sencilla, sería posible eliminar el 77 por ciento de las amenazas a la seguridad[13]. Es la incapacidad de Google y de sus socios de hacer que sus actualizaciones de seguridad estén ampliamente disponibles para su base de usuarios lo que brinda a los delincuentes el tiempo necesario para hallar agujero tras agujero en el sistema operativo de Android y decidirse a aprovecharlo.

Cuidado con las aplicaciones

Los fabricantes de aplicaciones como Rovio, Zynga y Snapchat no son los únicos que crean aplicaciones como modo de adquirir y vender tus datos; las mafias también han adoptado esta estrategia. Pese a que, por lógica, uno daría por entendido que cualquier aplicación enviada por un programador a las tiendas Android de Google o la App Store de Apple se someten a una concienzuda revisión en materia de seguridad tanto por lo que respecta a su código informático como a su desarrollador, no es oro todo lo que reluce. Con más de un millón de aplicaciones poblando los sistemas Android e iOS, prácticamente no se lleva a cabo ninguna verificación por parte de humanos, hecho que conocen bien los delincuentes, quienes han vulnerado las tiendas de aplicaciones para móviles en múltiples ocasiones. En su lugar, son algoritmos informáticos automatizados los que asumen toda la carga en el proceso de revisión, y los creadores de las tiendas de aplicaciones se limitan a esperar que haya suerte[14].

En consecuencia, los errores abundan y cada vez se albergan más aplicaciones que contienen *software* malicioso en lo que el usuario presume que es una tienda de aplicaciones fiable. En 2013 se detectó que más de 42 000 aplicaciones de la tienda Google contenían *software* espía y programas troyanos para robar información[15]. El *malware* de estas aplicaciones va dirigido específicamente contra los datos de tu teléfono, en especial la información financiera. Apenas unos días después de la inauguración de la tienda de aplicaciones Android Market, los delincuentes habían subido a ella aplicaciones de banca fraudulentas para las principales entidades bancarias de todo el mundo. Se trataba de aplicaciones con un alto grado de realismo, que, además, empleaban los logotipos correctos de los bancos, así como las tipografías y la gama cromática habitual de éstos, para mayor credibilidad. Decenas de miles de personas se descargaron aquellas aplicaciones y, al comprobar que no funcionaban, los clientes, enfadados, telefonearon a sus bancos, donde les informaron, para su asombro, de que «aún no tenemos aplicación para Android».

Los ciberdelincuentes han reestructurado sus operaciones para crear muchas otras aplicaciones bancarias falsas[16]. Mientras que en 2012 sólo se habían identificado sesenta y siete troyanos de banca, la cifra se había incrementado a más de mil trescientos hacia finales de 2013, de acuerdo con Kaspersky Lab. Hasta la fecha se han descubierto paquetes de *software* malicioso destinados a clientes de las principales entidades bancarias del mundo, incluyendo Citibank, ING, Deutsche Bank, HSBC, Barclays y otras sesenta y seis instituciones financieras del planeta[17].

Y el *malware* está más descontrolado aún en las tiendas de aplicaciones de otros fabricantes. Mientras que en el mercado de Android oficial existe al menos un apantallamiento algorítmico mínimo con respecto a la seguridad, en los sitios web externos no suele existir ningún tipo de control en absoluto. Como resultado de ello, se ha descubierto a más de quinientos vendedores de aplicaciones externos que ofrecen aplicaciones para Android con *software* malicioso[18]. Y puesto que en estas tiendas de aplicaciones no existen reseñas relativas a la seguridad, las aplicaciones

que contienen virus y troyanos pueden tener vidas útiles casi infinitas y proporcionar rentas de por vida a los delincuentes que las crean y las distribuyen.

Pese a ser mucho menos frecuentes, también se han descubierto algunos casos de aplicaciones maliciosas en la App Store de Apple[19]. Aunque el ecosistema del iOS de Apple está muy regulado y controlado, a muchos usuarios este entorno les resulta demasiado opresivo. Cuando adquieren inicialmente sus productos, los usuarios de iPhone no pueden personalizar el teclado, cambiar los navegadores por omisión, gestionar archivos localmente ni añadir *widgets* a sus pantallas de inicio, todas ellas funciones estándar en Android. Para superar tales limitaciones, muchos usuarios «liberan» sus dispositivos iOS empleando *software* especializado para vulnerar sus propios móviles y poder obtener acceso administrativo a la raíz del sistema y controlar funciones que Apple bloquea. Al liberar un dispositivo iOS, los usuarios obtienen acceso a miles de programas de *software* que carecen de la aprobación oficial de Apple. Cerca de diez millones de dispositivos iOS se han liberado y sus usuarios han accedido a tiendas de aplicaciones externas, como Cydia, para descargar sus *apps*[20]. Si bien al liberar estos dispositivos el usuario obtiene un control mucho mayor, también deja los dispositivos móviles iOS expuestos a las mismas amenazas de seguridad comunes en el ecosistema Android, incluidos diversos fraudes financieros.

¿Por qué necesita la aplicación de la linterna acceder a todos mis contactos?

Centenares de millones de usuarios de *smartphones* en todo el mundo se han descargado la popularísima y sumamente práctica aplicación de la linterna. Es tan práctica para buscar las llaves en el bolso o encontrar la cerradura de noche… y la mayoría de nosotros no hemos pagado nada por el privilegio de usarla. Pero ¿por qué necesita la aplicación de la linterna acceder a la agenda? ¿Por qué me pregunta cuál es mi localización? Mi localización debería ser evidente: estoy a oscuras, ¡por eso necesito una aplicación que simule una linterna! Resulta que la mayoría de estas aplicaciones, sobre todo para Android, son en realidad prácticos mecanismos para robarte datos, descargarse todos tus contactos, llevar un seguimiento constante de tu localización, instalar registradores de pulsaciones del teclado y hacerse con tu información financiera[21]. Lo que afrontamos, por consiguiente, es el uso de las aplicaciones para móviles como herramientas para cometer delitos, actos delictivos reducidos a la simplicidad de una *app* para teléfonos móviles.

Los permisos que garantizamos a estas aplicaciones, sobre todo en el ecosistema Android, donde no hay modo de denegar un permiso específico a una aplicación

concreta antes de instalarla, implican que tú y tus datos corréis riesgos. Los permisos para las aplicaciones en los dispositivos móviles son similares a los términos y condiciones: todos hacemos clic en «Aceptar» sin detenernos ni un instante a reflexionar sobre las implicaciones de nuestra decisión. La realidad es que otorgar esos permisos implica que el desarrollador de esa aplicación delictiva o fraudulenta obtiene la autorización necesaria para cometer un fraude o robarte de la cuenta bancaria mediante tu dispositivo móvil.

También hay delincuentes dedicados a crear aplicaciones fraudulentas destinadas específicamente a cometer fraudes de telecomunicaciones. Tres cuartas partes de todo el *malware* para teléfonos móviles que existe aprovecha las brechas en los sistemas de pago móviles para enviar mensajes SMS fraudulentos con tarifas prémium, cada uno de los cuales genera un beneficio inmediato de 10 dólares. Si multiplicamos esa cifra por los centenares de miles de mensajes SMS prémium falsos, el dinero generado es inmenso[22]. En un incidente, los estafadores lograron publicar versiones falsas de juegos extraordinariamente populares como *Angry Birds* y *Assassin's Creed* en una tienda de aplicaciones. Una vez descargada la aplicación, cada vez que el usuario la abría, enviaba tres mensajes SMS prémium sin el conocimiento del usuario a 7,50 dólares el mensaje. En cuestión de pocas horas, los ladrones acumularon decenas de miles de dólares con estos cargos fraudulentos[23].

Los teléfonos móviles secuestrados se utilizan cada vez más para enviar mensajes de correo electrónico no deseados al conectarse a las llamadas redes *botnets*[24] [*]. Las *botnets* son una colección de ordenadores infectados con *malware* y esclavizados que funcionan de manera simultánea bajo el control de piratas informáticos o delincuentes con el objetivo de enviar cantidades masivas de mensajes de correo electrónico no deseado o participar en ataques distribuidos de denegación de servicio (DDoS) sin el conocimiento del dueño legítimo del dispositivo. Si bien en el pasado las *botnets* estaban limitadas a ordenadores de sobremesa o portátiles, ahora los delincuentes y piratas informáticos se han apoderado del control de millones de teléfonos móviles y los han unido a sus «redes zombis», que crecen de manera exponencial[25]. Estas redes masivas de dispositivos pirateados se mantienen a la espera, listas para desatarse contra cualquier objetivo en cuanto se lo notifiquen. Dado que las ventas de dispositivos móviles están dejando rezagadas a las de ordenadores de sobremesa y portátiles en una proporción de diez a uno, no cabe duda de que el futuro de la informática está en los dispositivos móviles. Conscientes de ello, los delincuentes han imaginado que el futuro de la usurpación de datos, los DDoS y el *malware* también está en estos dispositivos móviles[26].

Incluso las aplicaciones legítimas pueden ponerte y poner tus datos en riesgo, si el *software* no está bien programado o contiene vulnerabilidades en materia de seguridad que no se han detectado. Tal fue el caso de la popularísima aplicación de «fotomatón social» conocida como Snapchat. Snapchat es un servicio que permite a los usuarios enviar autorretratos fotográficos (a menudo con cierto grado de

desnudez), los llamados «selfies», que supuestamente desaparecen al cabo de unos segundos de llegar al teléfono del destinatario. Se han enviado más de mil millones de fotografías mediante este servicio y, a finales de 2013, Facebook intentó sin éxito adquirir la empresa por tres mil millones de dólares. A principios de 2014 se reveló que Snapchat contenía un fallo de seguridad que había dejado expuestos a millones de usuarios de iPhone a ataques de denegación de servicio.

Esa vulnerabilidad implicaba que los piratas podían atacar tu teléfono enviando mil mensajes de Snapchat en sólo cinco segundos, a consecuencia de lo cual el teléfono se bloqueaba y no podía utilizarse hasta que se forzaba el reinicio del dispositivo[27]. Es más, los *hackers* también lograron vulnerar cerca de cinco millones de cuentas de usuario de Snapchat y publicaron una base de datos con los nombres de usuario y los números de teléfono en un sitio web de piratería informática[28]. Peor aún, se reveló que la función principal de Snapchat, la capacidad de enviar fotografías de desnudos que se autodestruirían en menos de diez segundos, también contenía errores[29]. Las imágenes no se autodestruían tal como se prometía, sino que podían recuperarse tanto en el dispositivo del destinatario como en los servidores informáticos de la propia Snapchat. Como resultado, decenas de miles de fotografías de Snapchat que supuestamente tenían que borrarse han aparecido en toda Internet y se han reposteado en Instagram y en numerosos sitios web de porno vengativo[30]. Las fotografías se han utilizado posteriormente con fines de extorsión y otros delitos.

Amenazas a las redes y a los dispositivos móviles

Las amenazas emergentes para los datos que transportamos en nuestros dispositivos móviles no sólo afectan a los consumidores, sino que además tienen un gran impacto en el sector. En las empresas de hoy en día, la llamada BYOD o (de «Bring Your Own Device» o «trae tu propio dispositivo») se ha convertido en la norma y brinda a los empleados acceso privilegiado a aplicaciones y datos corporativos sensibles desde sus dispositivos móviles personales. Hoy en día, el 89 por ciento de los empleados acceden a información relacionada con el trabajo desde sus teléfonos móviles y el 41 por ciento lo hacen sin el permiso de sus empresas[31].

Este fenómeno, devenido hoy en una práctica estándar en el puesto de trabajo, conlleva que la cantidad de información corporativa en riesgo aumenta a causa de los ataques *point and click* (o «de apuntar y hacer clic») lanzados con *software* espía contra los dispositivos móviles. Incluso cuando una red corporativa está bloqueada y protegida, los teléfonos móviles personales son un lugar del cual sustraer datos fácilmente. Las mafias no pierden el tiempo intentando piratear el lugar más seguro en el que has almacenado tu información; siempre van a por el eslabón más débil de

la cadena para obtener lo que quieren.

Los delincuentes se vuelven cada vez más inventivos a la hora de apuntar a la información de tu dispositivo móvil e incluso también a las redes telefónicas en sí. Por unos pocos cientos de dólares, pueden comprar y configurar una femtocelda, una estación base extensora de una red inalámbrica que mejora el servicio de los teléfonos móviles a los habitantes de las zonas que reciben señales de red pobres[32]. El dispositivo es una suerte de minitorre de telefonía móvil que los delincuentes pueden intervenir para hacer que tu móvil crea que es legítima cuando, en realidad, lo que hace es conectarse a una torre de telefonía móvil portátil bajo su control. ¿Con qué objetivo lo hacen? Con el de captar los datos que se envían desde tu teléfono, como la contraseña que tecleas para acceder a tu cuenta bancaria o correos electrónicos con información importante o comprometedora que puedas enviar. La femtoceldas fraudulentas pueden revestir una enorme utilidad para el espionaje industrial, ya que los piratas únicamente necesitan configurar el dispositivo fuera de las vallas perimetrales de la empresa para aprovecharse de los datos que emiten los dispositivos móviles de los centenares de empleados. Uno de los objetivos principales son los aeropuertos y los congresos importantes, donde se congregan multitud de empresarios. De manera que no eres tú el único que siente afinidad por los datos que guardas en tu teléfono inteligente.

Vulnerabilidad de los métodos de pago

Como es de suponer, los teléfonos móviles actuales se encuentran aún en sus estadios iniciales de desarrollo y multitud de sensores nuevos, como son la identificación de radiofrecuencias (RFID) y la comunicación de campo cercano (NFC), los dotarán de nuevas funcionalidades, y también de nuevas vulnerabilidades. Uno de los ámbitos en los que esto es más fácil de apreciar es en la desaparición de las divisas físicas. El futuro del dinero es móvil y virtual y ya existen multitud de aplicaciones y sensores nuevos a la espera de reemplazar tu billetero y el dinero en efectivo que llevas en el bolsillo. De hecho, algunos proveedores de telefonía móvil, como Safaricom en África, despuntan en el panorama general de los pagos. En Kenia, por ejemplo, el 25 por ciento del PNB nacional se gestiona mediante transacciones a través del sistema de pagos M-PESA de Safaricom[33]. Los sistemas móviles de transferencia de dinero, inexistentes a finales del siglo XX, ahora están disponibles en otros setenta países y se emplean para transferir miles de millones de dólares mensuales[34]. En concreto, han resultado sumamente prácticos para conseguir que las poblaciones del mundo en desarrollo, que hasta ahora carecían de cuentas bancarias, accedan al mundo global del comercio, con una repercusión positiva importante para las economías locales.

En el mundo desarrollado, también se ha pisado el acelerador para adoptar y desplegar sistemas de pago mediante telefonía móvil. MasterCard y Visa han puesto en funcionamiento numerosos programas de pago NFC que permiten a los usuarios ya sea abrir una aplicación en sus teléfonos móviles, ya sea pasar por encima o acercar el dispositivo a un sensor sin contacto (conocidos como *contactless*) para cobrar bienes y servicios de manera rápida. Desde Starbucks hasta Best Buy pasando por los parquímetros de San Francisco y los taxis en Nueva York, el pago mediante chips sin contacto se está convirtiendo en el método de pago rápido preferido por los usuarios. Pese a que Google fue una de las primeras empresas en adoptar sistemas de pago NFC para sus teléfonos Android, en septiembre de 2014 Apple se subió al tren e incorporó la tecnología «Desliza y cobra» a su último lote de teléfonos iPhone. En el ecosistema Android, el sistema de pago Wallet de Google permite a los usuarios guardar la información de sus tarjetas de debito y crédito en Google y abrir la aplicación Wallet para finalizar el pedido en un número creciente de comercios mediante cualquier terminal en tienda que tenga habilitado PayPass. Google Wallet funciona con los chips NFC en diversos teléfonos móviles, tanto HTC como LG, Motorola y Samsung[35].

El dinero, tal como se representa en estos dispositivos móviles, no es más que datos, datos que se almacenan en aplicaciones vulnerables, controladas por sistemas operativos profundamente vulnerables, que utilizan tecnologías de sensores y protocolos de transferencia de datos mediante sensores poco seguros. ¿El resultado evidente? El futuro del dinero móvil también podría ser el dinero de los «carteristas» móviles. El sistema Google Wallet ya ha sido vulnerado por delincuentes en numerosas ocasiones y aplicaciones como Wallet Cracker permiten a cualquiera ver a su antojo el número del código de identificación personal (PIN) que un usuario utiliza para acceder a él. Es más, si un usuario pierde o si le roban su teléfono Android, la persona que lo encuentra o lo hurta puede gastarse con toda tranquilidad el dinero que el usuario tenía almacenado en su Google Wallet (datos en el dispositivo) en cualquier tienda[36]. Con el auge de las aplicaciones NFC y la destacable irrupción de Apple en el mundo de los pagos mediante móvil, sin duda comprobaremos cómo la atención de los *hackers* se concentra cada vez más en estos sensores y en otros insertados en los dispositivos móviles, incluido el GPS.

Tu localización es la escena del crimen

Los anunciantes y agentes intermediarios de datos no son los únicos interesados en llevar un seguimiento constante de tu localización. Delincuentes, estafadores y acosadores también han descubierto la practicidad del chip GPS que incorporan los teléfonos inteligentes. A menudo a los *hackers* les basta con aprovechar el diligente

trabajo realizado por los agentes intermediarios de datos como medio de subvertir los datos que filtras. Pongamos, por ejemplo, la aplicación de relaciones esporádicas basada en tu localización, Tinder, que ya hemos analizado en el capítulo 4. Habida cuenta de los volúmenes de datos, fotografías lascivas y potenciales parejas para mantener relaciones sexuales que maneja, no sorprende que los piratas informáticos se empeñaran en descubrir una vulnerabilidad en la seguridad de la aplicación que permitiera a todo el mundo descubrir en tiempo real la localización de los usuarios situados en un radio de metro y medio, una información concebida para mantenerse en privado[37]. En el mejor de los supuestos, el uso de dichos datos acerca de la ubicación desemboca en un encuentro fortuito positivo. En el peor de los casos, los datos sobre la localización generados por aplicaciones fraudulentas como Girls Around Me podrían demostrar ser una herramienta atroz en manos de acosadores, violadores y posibles pederastas. De hecho, en 2012, la policía del sur de Australia advirtió a la población que los pedófilos estaban utilizando los datos de geoetiquetaje incrustados en las fotografías de niños publicadas en Internet para dar con posibles objetivos[38].

El uso de estos datos con efectos adversos en casos de discordia en relaciones y violencia doméstica está cada vez más extendido. En 2012, el Departamento de Justicia de Estados Unidos reveló que cada año se registraban 3,4 millones de víctimas de acoso, de las cuales centenares de miles eran sometidas a seguimiento mediante *software* espía y vulneraciones de sus GPS[39]. Bienvenido al mundo de la vigilancia «de apuntar y hacer clic». Cabe aclarar que utilizar este *software* espía supone una intromisión ilegítima de acuerdo con las leyes federales estadounidenses y se considera ilegal, pero las herramientas están ampliamente disponibles incluso para los *hackers* novatos… o para exparejas sin experiencia previa. Mobile Spy, a título de ejemplo, convierte cualquier teléfono en un dispositivo de vigilancia oculto, pues permite grabar los sonidos ambientales de los alrededores incluso aunque no se esté efectuando una llamada. La empresa también fabrica un producto «para monitorizar el iPad» y todo su *software* incluye un modo de «cámara oculta» que permite a terceras partes activar de manera remota tu cámara y supervisar lo que ve en tiempo real, además de guardar en un servidor central aquellas fotografías o vídeos que elijan tomar con tu dispositivo para su posterior descarga. El asesino convicto Simon Gittany, un novio celoso y maltratador, utilizó en 2011 otro producto en el mercado, Mobistealth, para monitorizar la actividad del teléfono móvil de su prometida, Lisa Harnum, en Sídney, Australia. De este modo, cuando Harnum envió a una amiga un SMS haciéndole la confidencia de que tenía previsto abandonarlo, porque la maltrataba, Gittany recibió una notificación instantánea a través de Mobistealth de la intención de su novia en su propio teléfono móvil. Enfurecido por los planes de ella, condujo hasta casa de Harnum y, en el altercado que siguió, la arrojó desde el balcón de su apartamento, situado en la decimoquinta planta de un edificio[40].

Ahora bien, en algunos casos, los maltratadores dentro de la pareja ni siquiera necesitaron incorporar *software* espía de terceras partes a un teléfono: se limitaron a activar el programa familiar de AT&T FamilyMap que la operadora de telefonía inalámbrica ofrece a modo de servicio y permite al propietario de una cuenta de teléfono móvil llevar un seguimiento de todos los dispositivos incluidos en su plan[41]. Mediante el servicio de mapeo de familiares inalámbrico que ofrece la operadora, Andre Leteve, de Scottsdale, Arizona, logró localizar a su esposa, que lo había abandonado y se había llevado a sus dos hijos con ella, y los asesinó[42]. En la actualidad, ni siquiera es preciso pagar un servicio de tales características a proveedores como AT&T, ya que estas funcionalidades se incorporan tanto en los dispositivos iOS como Android, con servicios con nombres como «Buscar a mis amigos» o «Buscar mi teléfono», que pueden activarse a distancia para rastrear a otras personas[43]. Para combatir tales amenazas, las casas de acogida para mujeres maltratadas solicitan a las recién llegadas que les entreguen sus teléfonos en el mismo momento de la admisión, les quitan la batería y los desensamblan para evitar que sirvan de faro a los posibles maltratadores[44]. Sin embargo, el hecho de compartir su localización no sólo debe preocupar a las víctimas de la violencia doméstica, sino que también los soldados en el campo de batalla deben tener en cuenta que los terroristas pueden monitorizar sus actividades en línea para establecer potenciales vías de ataque.

«¿Una medalla en Foursquare o un pasaporte a la otra vida?», es la pregunta que actualmente formula el Ejército de Estados Unidos a sus soldados[45]. Y no se trata de ninguna pregunta retórica, si tenemos en cuenta que los terroristas aprovechan los datos geoetiquetados. Por ejemplo, cuando las fuerzas militares estadounidenses recibieron una nueva flota de helicópteros Apache AH-64 en su base en Irak, algunos soldados desplegados publicaron autorretratos posando frente a los nuevos aparatos en Facebook. Desconocían que sus teléfonos incrustaron por accidente sus coordenadas de GPS en las fotografías. Los insurgentes no sólo monitorizaban las publicaciones en Facebook de los soldados, sino que se descargaban las fotografías y las analizaban para obtener datos de espionaje útiles. La información acerca de la longitud y latitud incorporada a aquellas fotografías permitió a los terroristas lanzar una serie de ataques de precisión con mortero que destruyeron cuatro de los nuevos Apaches llegados a las instalaciones[46].

No sólo es posible localizarnos mediante los datos que filtramos a través de nuestros teléfonos móviles o los archivos incrustados, como fotografías y vídeos, sino que cada vez filtramos más los datos de nuestra localización en el mundo físico. Los dispositivos de vigilancia oculta con GPS son baratos de adquirir en Internet e incluso están a la venta en la ubicua revista *SkyMall* disponible en todos los vuelos que realizamos. En dicho catálogo, Tracking Key vende un dispositivo de vigilancia GPS que se acopla mediante un imán o Velcro a cualquier vehículo y permite a los propietarios del dispositivo reproducir en un mapa en línea todos los puntos a los que

ha viajado dicho vehículo, además de conocer la velocidad a la que se desplaza, determinada en intervalos de un segundo[47]. «Útil para comprobar si tu hijo conduce con exceso de velocidad, adónde va tu cónyuge o adónde viajan tus empleados». En el pasado, únicamente una agencia de espionaje o el FBI habrían tenido acceso a un dispositivo de alta tecnología de estas características, pero ahora, dado el descenso exponencial de los precios de esta tecnologías, incluso una madre de familia puede espiar a sus hijos o controlar a su marido, si sospecha que la engaña.

En el mundo de los datos masivos, incluso podemos filtrar nuestra localización física sin un teléfono móvil con vigilancia oculta o un rastreador GPS acoplado a nuestro vehículo. Una nueva tecnología, conocida como reconocimiento automático de matrículas (ALPR en sus siglas en inglés), permite tanto a los gobiernos como a las personas normales utilizar cámaras de vídeo y el reconocimiento de caracteres óptico para registrar las ubicaciones de los vehículos cuando avanzan desde un punto con cámara hasta otro y conocer el movimiento en tiempo real de cualquier vehículo a través de una ciudad o país con un grado de detalle enorme. De Minnesota a Nueva Jersey y de Ankara a Sídney se han registrado cientos de millones de matrículas reconocidas[48]. Ello permite formular preguntas a estas bases de datos masivas para determinar la posición de cualquier vehículo a lo largo del tiempo. Un dato interesante es que aquellas personas a quienes se fotografía no pueden ser acusadas ni consideradas sospechosas de ninguna infracción en una abrumadora mayoría de los casos, pero ello no obsta para que los datos se almacenen, pues podrían resultar útiles para investigaciones delictivas en algún momento futuro.

También se están instalando unidades ALPR en los coches patrullas e incluso en grúas, con lo cual la policía y los servicios municipales están ampliando enormemente sus bases de datos. Empresas privadas como Digital Recognition Network en Texas o MVTRAC en Illinois están elaborando bases de datos masivas con los datos de las ALPR, que luego venden a los agentes del sector de recuperación de vehículos[49]. De este modo, si alguien se retrasa en sus pagos, estas empresas conocen todas las ubicaciones en las que ha estado el vehículo y pueden enviar una grúa a recuperarlo. Del mismo modo que los coches de Google Street View conducen por las calles de nuestras ciudades grabando en vídeo todo lo que ven, también lo hacen las empresas de ALPR privadas. Su objetivo es rastrear tu vehículo y localizarlo delante de tu hogar, en tu lugar de trabajo o en los comercios donde compras. Por supuesto, estos datos también se monetizan, una práctica que, en 2014, era completamente legal. Ahora bien, a medida que broten como setas estas bases de datos masivas de reconocimiento de matrículas, también lo harán los delincuentes que las utilicen y los consiguientes riesgos para la privacidad.

Y si Experian y Acxiom pueden sufrir hurtos de datos o vender sus conjuntos de datos a organizaciones criminales, ¿por qué tendrían que ser distintos los comerciantes de ALPR? De ahí que incluso las víctimas de la violencia doméstica que no tienen presencia en Internet y ni siquiera llevan teléfonos móviles puedan ser

rastreadas allá donde conduzcan sus vehículos. Hemos visto cómo los datos de ALPR se utilizaban de manera indebida en el pasado, ya en 1998, cuando un teniente de policía de Washington, D. C., utilizó su sistema informático para identificar a los propietarios de los vehículos aparcados en el estacionamiento de un popular bar gay local. Luego empleó dichos datos para extorsionarlos, amenazándolos con sacarlos del armario, a menos que le pagaran un soborno[50]. Si bien la naturaleza de las amenazas vinculadas con los datos de ALPR puede haber cambiado en la actualidad, lo cierto es que siguen existiendo. ¿Cómo puede utilizarse esta información en casos de divorcio (su coche estaba aparcado frente a la casa de otra mujer)? ¿Cómo pueden emplearlas los seguros médicos (vemos su coche aparcado frente a un bar cinco días a la semana)? Y existen riesgos adicionales: los sistema ALPR no son infalibles en el reconocimiento de matrículas y los errores pueden derivar en graves consecuencias. En 2009, varios coches patrulla detuvieron el vehículo de una mujer de cuarenta y siete años en San Francisco y, a punta de pistola, seis oficiales la hicieron descender de él… todo porque el sistema ALPR había leído mal un dígito de su matrícula y había etiquetado su vehículo como robado, cuando la mujer se dirigía, sencillamente, a hacer la compra al supermercado[51].

Incluso los comerciantes al por menor han empezado a hurtar nuestros datos de localización de modos nuevos e imprevistos. El centro comercial Nordstrom, por ejemplo, recientemente ha empezado a llevar un seguimiento de sus clientes a través de las señales de Wi-Fi y las direcciones MAC de sus teléfonos inteligentes cuando compran en sus tiendas. Al desplazarte por sus comercios, Nordstrom puede seguirte digitalmente para comprobar cuánto tiempo pasas en la sección de ropa interior femenina y cotejarlo con el que inviertes en la sección de calzado masculino. Este comercio de lujo contrató a Euclid, una empresa especializada en ayudar a los comerciantes a rastrear los movimientos de sus clientes mediante las conexiones Wi-Fi habilitadas en sus comercios. Hasta la fecha, Euclid ha tomado las huellas digitales y rastreado más de cincuenta millones de dispositivos móviles en las cuatro mil ubicaciones que tienen este servicio habilitado, incluidos centenares de comercios estadounidenses, como Home Depot (en efecto, la misma empresa que filtró cincuenta y seis millones de tarjetas de crédito por una vulneración de datos en septiembre de 2014 ahora se propone recopilar más datos acerca ti y tus localizaciones en el seno de sus establecimientos[52]). Ante la ausencia de toda regulación de este fenómeno, la compras bajo vigilancia acabarán convirtiéndose en la norma, y la tecnología se orienta de manera creciente a rastrear a las personas sin conexión en espacios reales.

En Nordstrom, las únicas notificaciones que se daban a los clientes acerca del uso de la nueva tecnología de rastreo era un pequeño cartel bien escondido y apenas visible colocado a la entrada a los establecimientos. El texto del cartel aclaraba que se trataba de un modelo con cláusula de opción, lo cual significaba que, si no querías participar, tenías dos opciones: no entrar en las tiendas o apagar el teléfono móvil.

Los datos obtenidos de servicios como éste pueden almacenarse y, de hecho, se almacenan para siempre. Como resultado de ello, el abogado de divorcio de tu cónyuge podría citar a Nordstrom o Euclid para comprobar si tú y tu amante estabais en la misma tienda comprando juntos intimidades. O tu jefe podría contratar a un agente intermediario de datos para averiguar dónde estabas el día que telefoneaste para decir que te encontrabas mal: «Si tan enfermo estabas, ¿qué hacías (con tu teléfono móvil) en el cine y en Hooters esa tarde?». Y lo que es aún peor, los delincuentes podrían acceder a toda esta información a lo largo del tiempo mediante la clandestinidad digital y utilizarla para chantajear, estafar o acosar a los objetivos de su elección.

Incluso Disneylandia, el «lugar más feliz del mundo», se está volcando en las tecnologías basadas en la localización para hacer un seguimiento de sus clientes mediante unas pulseras llamadas MagicBands, dispositivos con chip identificador de radiofrecuencias (RFID) incorporado que permiten a Disney seguir la pista a sus clientes por todos sus parques temáticos. El objetivo es utilizar los datos masivos para que disfrutes (y gastes) al máximo durante tu estancia en el Reino Mágico. Y tras Disney, es probable que vengan otros y que estas tecnologías de rastreo humano se desplieguen también en casinos, centros vacacionales e incluso en aeropuertos en el futuro.

Pronóstico: nubosidad variable

Al tiempo que nuestros dispositivos móviles filtran cantidades descomunales de datos, cada vez afloran más riesgos relacionados con los datos masivos del mundo de la «informática en la nube». La «nube» alude a la gigantesca red de recursos computacionales disponibles en Internet y a la práctica de utilizar tales servidores remotos para almacenar, gestionar y procesar la información del mundo. El paradigma en el ámbito de la informática ha cambiado: ahora cada vez almacenamos menos información de manera local en nuestros ordenadores y, en su lugar, la guardamos en cualquier otro punto del planeta. Ya prácticamente no compramos programas informáticos, sino que los alquilamos o los recibimos gratis al usar un nuevo modelo de negocio conocido como *Software* como un Servicio (ScuS).

En el frente personal, la nube implica que Google almacena nuestro correo electrónico; Instagram, nuestras fotografías, y Dropbox, nuestros documentos…, por no mencionar lo que los teléfonos móviles cargan automáticamente en la nube en nuestro nombre. En el mundo corporativo, los clientes empresariales no sólo utilizan Dropbox, sino que han externalizado funciones empresariales fundamentales que en el pasado se habrían gestionado de manera interna a proveedores de ScuS como Salesforce.com, Zoho.com y Box.com. Desde la perspectiva de los delitos y la

seguridad, la acumulación de todos estos datos, medidos en exabytes, significa que nuestra información más personal ya no se almacena exclusivamente en nuestros discos duros, sino que ahora se agrega a servidores informáticos distribuidos por todo el planeta. Al incorporar en servidores informáticos alojados en la nube los datos importantes de todo el mundo, tanto financieros como de otro tipo, les hemos ahorrado a los delincuentes la necesidad de poner el blanco en el disco duro de cada persona y, en su lugar, hemos guardado todas las joyas en un mismo sitio para que afinen la puntería (recuerda a Willie Sutton y su pasión por los bancos).

Y la nube ha venido para quedarse[53]. A estas alturas, ya no hay vuelta atrás. A principios de 2014, Google redujo el precio de sus ofertas de almacenamiento en la nube en cerca de un 70 por ciento, con una tarifa de sólo 0,026 dólares por gigabyte al mes (algo menos de tres centavos, frente a los 437 000 dólares que costaba en 1980). Aquel movimiento causó un terremoto en todo el sector y desencadenó una guerra de precios con otros gigantes del almacenamiento en la nube, como Amazon y Microsoft. La disponibilidad de recursos informáticos tan baratos y el creciente abanico de ofertas de ScuS tendrán repercusiones positivas inimaginables en la productividad personal, el mundo empresarial y la innovación, lo cual a su vez acelerará la inevitable transición a la computación en la nube. No obstante, este traslado de todos los datos disponibles a la nube conlleva riesgos adicionales. Piensa en los grandes ciberataques acaecidos hasta la fecha: Target, Heartland Payment Systems, TJX y Sony PlayStation Network. El robo de estos centenares de millones de cuentas fue posible debido a que los datos estaban almacenados en una única ubicación virtual. La nube es tan práctica para los internautas como para las empresas… y los delincuentes. Para lidiar con estos riesgos, se han instituido organizaciones sin ánimo de lucro, como Cloud Security Alliance, con el fin de fomentar las mejores prácticas y mejorar la seguridad en la época de la computación en la nube.

La virtualización y el almacenamiento de todos estos datos son extremamente complejos y plantean un amplio abanico de problemas legales, de seguridad y de políticas públicas. En primer lugar, ¿dónde exactamente almacena mis datos esta nube mágica? La mayoría de los usuarios no tienen ni idea de en qué lugar del mundo se guardan sus datos cuando cambian su estado en Facebook o cargan una fotografía en Pinterest. El hecho de que ni siquiera nos detengamos a cuestionárnoslo da fe de la practicidad (y opacidad) del sistema. Sin embargo, desde la perspectiva de los riesgos personales y de la dirección de empresas, el hecho de que los datos se almacenen en Estados Unidos, Rusia, China o Islandia sí comporta diferencias.

Los perímetros corporativos e individuales que solían salvaguardar nuestra información internamente están desapareciendo y el principio y el final de nuestras redes informáticas se está desdibujando. Cada vez resulta más difícil comprobar qué datos entran y salen de una empresa, y tal labor resulta prácticamente imposible en el ámbito personal. La transición a la nube comportará un cambio de las reglas del juego

en materia de seguridad porque redefine íntegramente dónde se almacenan y transfieren los datos y dónde se accede a ellos, y crea nuevas oportunidades de amplio alcance para los *hackers* y delincuentes. Es más, el almacenamiento de nuestros datos en un servidor externo plantea interrogantes relevantes relativos a nuestra honda dependencia de los sistemas de información alojados en la nube. Cuando dichos servicios quedan inhabilitados o no están disponibles como resultado de un ataque de denegación de servicios (DDoS) o cuando nos quedamos sin conexión a Internet, no disponemos de acceso a nuestros datos y el negocio se paraliza.

Tal como descubrió Mat Honan, confiar información personal valiosa, como las fotografías de los hijos y años de mensajes de correo electrónico, a proveedores de servicios en la nube conlleva sus riesgos particulares. Todos los grandes proveedores de servicios en la nube han sido objeto de ataques remotos perpetrados por delincuentes, incluidos entre ellos Dropbox, Google y Microsoft, y es de esperar que se produzcan otros nuevos en el futuro[54]. En efecto, varios años después de que Honan sufriera un ataque y publicara un artículo en el que suplicaba «acabar con las contraseñas» dada su total ineficacia, miles y miles de personas y empresas continúan viendo cómo se vulneran sus cuentas alojadas en la Red y cómo se hurtan sus datos, incluidas entre las víctimas varias actrices de primera línea de Hollywood. A finales de 2014 se robaron centenares de fotografías (muchas de ellas de una naturaleza absolutamente íntima y con desnudos) a celebridades como Jennifer Lawrence y Kate Upton, en un ataque perpetrado por unos piratas informáticos que lograron subvertir los nombres de usuario, contraseñas y preguntas de seguridad que protegían las cuentas de iCloud de Apple de las actrices[55]. Si bien el ataque puede estar dirigido contra el proveedor de servicios en la nube, la víctima final acaba siendo el usuario y los datos que se sustraen son los suyos. Como es de prever, los derechos reservados en los términos de servicio conllevan que las empresas asumen poca o nula responsabilidad cuando se vulneran los datos. Estos ataques amenazan la propiedad intelectual, los datos de los clientes e incluso información gubernamental comprometida.

En 2008, las especificaciones del diseño de alto secreto del helicóptero del presidente de Estados Unidos, el Marine One, se hallaron en Internet, a disposición de cualquiera, alojadas en una red de pares (P2P) en Irán. Las redes P2P permiten compartir fácilmente archivos descentralizados y suelen vincularse con la distribución de películas y música pirateada en la clandestinidad digital. ¿Cómo acabaron los planes de alto secreto y las funcionalidades de uno de los helicópteros tecnológicamente más avanzados del mundo en manos de los iraníes? Muy sencillo. Una contratista militar con sede en Bethesda, Maryland, que trabajaba en el proyecto del Marine One decidió que le apetecía escuchar música gratis en su ordenador portátil del trabajo. Cuando descargó el popular *software* de compartición P2P, instaló de manera accidental y sin saberlo el programa en el directorio equivocado de su

ordenador. Por tal razón, los planos y las funciones de seguridad defensiva del helicóptero militar que traslada al presidente de Estados Unidos desde la Casa Blanca al Air Force One se filtraron en las redes de compartición de música P2P de todo el mundo, incluidas las alojadas en Irán[56]. Por querer escuchar música gratis, un proyecto militar valorado en miles de millones de dólares quedó vulnerado y los planos del helicóptero Sikorsky VH-3D del Presidente acabaron en una red de pares de Irán, albergados junto a canciones pirateadas de Michael Jackson y Shadmehr Aghili, el rey indiscutible del pop persa. Al ser interrogado tanto por el FBI como por el Departamento de Defensa de Estados Unidos, el antiguo contratista militar admitió su error, pero, para entonces, los daños eran irreparables. Nuestras interconexiones a escala planetaria y el almacenamiento infinito de un volumen cada vez mayor de datos implica que las filtraciones son prácticamente inevitables. ¿Qué datos podrías estar filtrando tú o tu empresa en la nube?

Grandes datos, Gran Hermano

Un dato interesante es que los gobiernos no sólo son víctimas de las filtraciones de datos, sino que en gran medida las provocan. La información es el motor de todas las operaciones de espionaje y los gobiernos de todas las envergaduras están plenamente focalizados en los datos masivos. No sólo los chinos piratean el mundo, también lo hacen los estadounidenses, británicos, rusos, australianos, canadienses, sirios, israelíes, egipcios, iraníes e incluso etíopes. De hecho, hay más de cien países con programas de *hackeo* informático ofensivos en activo, aunque quizá no tan amplios como los del gobierno y la Agencia de Seguridad Nacional (NSA) de Estados Unidos[57]. Se dice que la NSA intercepta y almacena más de 1700 millones de mensajes de correo electrónico, llamadas telefónicas y SMS al día, lo cual le ha permitido compilar una base con cerca de 20 billones de transacciones de datos desde los atentados contra las Torres Gemelas del 11-S[58]. La agencia cataloga quién telefonea a quién, quién envía mensajes de correo electrónico a quién y quién transfiere dinero a quién.

Con todo, dada la expansión exponencial de estos almacenes de datos masivos, la agencia de espionaje electrónico se está quedando sin espacio de almacenaje[59]. Para solventar este contratiempo, el gobierno de Estados Unidos se halla en proceso de construir unas nuevas instalaciones operativas gigantescas en pleno desierto de Utah, las cuales permitirán a la NSA guardar en memorias intermedias y procesar 100 000 veces más datos de los que actualmente contiene la Biblioteca del Congreso[60]. Y eso no es más que el principio…

Las revelaciones de Edward Snowden han documentado la amplitud de las

canalizaciones de datos que lleva a cabo la NSA, incluidos los montones imparables de datos acerca de nuestra localización y redes sociales que todos generamos. Si bien la lista completa de las revelaciones de Snowden es demasiado extensa para resumirla aquí, un análisis de las más destacadas reveladas hasta la fecha debería dejar claro que el sector privado no está sólo en su persecución agresiva de datos masivos. El programa PRISM de la Agencia de Seguridad Nacional estadounidenses permitía al gobierno recopilar volúmenes ingentes de datos de empresas como Microsoft, Google, Facebook, Skype, AOL y Apple, inclusive mensajes de correo electrónico, vídeos, fotografías, actualizaciones de estado y ubicaciones de los usuarios[61].

Snowden también reveló que la NSA accedía a y descargaba las conexiones interpersonales entre los usuarios de las redes sociales (quién hablaba con quién, con qué frecuencia y cuáles eran sus ubicaciones), incluidos los gráficos de la redes sociales de los ciudadanos estadounidenses[62]. A estos gráficos de redes se añadían millones de agendas y listas de contactos de los usuarios en línea que la agencia también compilaba[63]. De esta manera, cuando eliges utilizar Google Contacts o iCloud para almacenar datos personales de tus amistades, familiares o socios empresariales, se convierten en presa fácil de terceros, incluidos gobiernos.

La NSA no sólo había establecido relaciones de cooperación con empresas estadounidenses, sino que también las ponía en su punto de mira cuando lo consideraba oportuno, inclusive a Google y Yahoo!, en cuyos centros de datos la agencia de espionaje se infiltraba sin autorización[64]. Utilizando las mismas técnicas básicas que emplean los piratas informáticos y las mafias y delincuencia organizada, la NSA infectó más de cincuenta mil redes informáticas en todo el mundo mediante *software* malicioso con el fin de obtener acceso a objetivos de su interés[65]. La agencia incluso fingió ser Facebook en numerosos ataques con «intermediario» con la pretensión de llevar el seguimiento a determinados individuos en las redes sociales[66]. Mediante esta técnica, los objetivos de su interés se conectaban a una réplica del sitio de Facebook controlada por el gobierno, cosa que permitía a la agencia instalar *software* malicioso en sus ordenadores.

Pero la NSA no hizo todo eso por sí sola, sino que cooperó con organizaciones hermanas, como su equivalente británico, los Government Communications Headquarters. Juntos, ambos organismos participaron en el programa «Optic Nerve», que interceptó millones de chats de vídeo de Yahoo! asumiendo el control de las cámaras de vídeo de los ordenadores portátiles de los usuarios y tomando fotografías cada cinco minutos[67]. Se almacenaron así millones de imágenes, incluido un gran número de imágenes sexualmente explícitas con desnudos. Lo más alarmante es que muchos de los chats de vídeo interceptados correspondían a personas desvinculadas de cualquier operación de espionaje o inteligencia, por el mero hecho de que era más sencillo hacerse con todos los chats que clasificar uno por uno cuáles eran los que interesaban.

La NSA también replicó las técnicas ya probadas por los anunciantes y comerciantes y sus operaciones de recopilación de datos comerciales. Por ejemplo, la agencia de espionaje creó e instaló *cookies* de rastreo en discos duros y teléfonos móviles para grabar las localizaciones y los hábitos en línea de las personas vigiladas[68]. De acuerdo con Snowden, la NSA incluso pinchaba aplicaciones para *smartphones*, como *Angry Birds* de Rovio[69]. La agencia de espionaje reconoció que *Angry Birds* ya estaba realizando un trabajo tan magnífico en el hurto de datos que no necesitaba duplicar esfuerzos. En su lugar, se limitó a interceptar las colosales cifras de datos que enviaban a Rovio quienes creían, ingenuamente, que el único cometido de la aplicación era lanzar pájaros a unos cerdos verdes risueños por mera diversión.

Sólo un ínfimo porcentaje de los mil setecientos millones de usuarios de *Angry Birds* entendía que la aplicación «gratuita» compartía con Rovio datos que implicaban desde su localización constante hasta su orientación sexual. Sin embargo, nadie, ni siquiera la propia empresa artífice de la aplicación, sabía que estaba proporcionando dichos datos (sin querer, desde luego) a la NSA[70]. De hecho, algunos analistas de la NSA se dedicaban a utilizar las amplísimas herramientas de espionaje de la agencia para espiar a sus novios, novias, cónyuges y examantes. Se documentaron numerosas infracciones por las cuales funcionarios de la NSA se infiltraron en las direcciones de correo electrónico y números de teléfono de otras personas para leer sus mensajes, conocer su ubicación y escuchar a hurtadillas sus llamadas telefónicas[71]. Los actos de estos empleados plantean la cuestión proverbial a la par que importantísima de quién vigila a quienes nos vigilan.

Si bien una mayoría abrumadora de los objetivos de la NSA parecen encontrarse en puntos transoceánicos, docenas de servicios de seguridad de todo el mundo utilizan el espionaje electrónico para vigilar y reprimir a su población nacional. En China, Irán, Egipto, Siria y Bahréin, entre otros, los datos almacenados en la red se supervisan e interceptan de manera rutinaria por motivos de espionaje político y con vistas a mantener el *statu quo*. La mayoría de los países no construyen estos sistemas de vigilancia, sino que los adquieren a empresas ubicadas en el extranjero, como la alemana Gamma International, artífice del paquete de vigilancia electrónica FinFisher. FinFisher permite a los servicios de inteligencia nacionales monitorizar a miles de objetivos de manera simultánea a través de sus móviles, redes sociales y actividades en Internet[72].

Una vez se han establecido estos sistemas de vigilancia de datos masivos, pueden utilizarse para hacer el bien común, como, por ejemplo, para abortar un ataque terrorista inminente, o en detrimento común, como para represaliar y hostigar a activistas defensores de los derechos humanos y subvertir procesos democráticos. Si bien las redes sociales fueron de una ayuda inestimable para los disidentes de Egipto y Túnez durante la Primavera Árabe, acontecimiento que recibió una tremenda difusión en la prensa de todo el mundo, la moneda de las redes sociales también tenía otra cara. Los millones de tuits y publicaciones en Facebook también proporcionaron

herramientas sumamente útiles a los gobiernos para perseguir a los disidentes. La organización de una manifestación a través de Facebook garantiza al gobierno un acceso sin obstáculos a los planes de los opositores, y prácticamente todos los Estados cuentan con las habilidades requeridas para aprovechar esos datos filtrados.

Con ocasión del alzamiento contra Bashar al-Assad iniciado en 2011, el gobierno sirio, con asistencia y soporte técnico de Irán, desplegó una amplia gama de programas para monitorizar los sitios web de redes sociales como Facebook y Twitter con el objetivo de rastrear las comunicaciones entre las figuras destacadas de la oposición[73]. Los líderes del movimiento contrario a Assad identificados online se han marcado como objetivos de ataque, y lo mismo ha ocurrido con sus familiares. En los días postreros del expresidente ucraniano Víktor Yanukóvich, sus fuerzas gubernamentales demostraron el poder de la tecnología para represaliar e intimidar a las fuerzas de la oposición. Cuando los manifestantes se congregaron en las calles de Kiev, el gobierno ucraniano detectó las localizaciones de todos los teléfonos móviles en las proximidades de los enfrentamientos callejeros entre los agentes de policía antidisturbios y los manifestantes. Los teléfonos móviles (y sus dueños) fueron identificados en tiempo real y recibieron el que podría considerarse «el mensaje de texto más orwelliano enviado nunca por un gobierno: “Querido suscriptor, estás registrado como participante en un disturbio público”»[74]. Las palabras se escogieron con esmero, pues Yanukóvich ya había declarado ilegal tal participación en los días previos y cualquiera que hubiera transgredido su ley era susceptible de ser arrestado sin tardanza.

El lado oscuro de los datos masivos

El legado de los datos masivos que se perfila en el horizonte bien podría ser el de la vigilancia a todas horas, la abolición de la privacidad y un sinfín de amenazas delictivas hasta ahora inconcebibles. Las redes sociales, los teléfonos inteligentes, las aplicaciones móviles, la nube y toda una serie de tecnologías adicionales no sólo conllevan que Nordstrom, Acxiom, Facebook y Google puedan localizarte cuando lo deseen, sino que también puedan hacerlo los Zetas, Lashkar-e-Toiba, maltratadores y acosadores. No obstante, lo que la mayoría de las personas no entiende es que cualquier dato recopilado acabará filtrándose, invariablemente. Los sistemas informáticos actuales son demasiado inseguros como para almacenar a buen recaudo los volúmenes de información que generamos.

Hasta la fecha, la principal amenaza contra los datos masivos han sido su robo y filtración. Sin embargo, eso no era más que el principio. A medida que avancemos, toparemos con nuevos riesgos que podrían demostrar ser incluso más peligrosos, como la modificación sin autorización de la información de la cual depende el mundo

para llevar a término sus actividades diarias. Aunque hemos depositado una confianza tremenda en los datos que guardamos febrilmente en ubicaciones externas, la precisión subyacente de esta información, tal como descubriremos, puede subvertirse con suma facilidad, con consecuencias relevantes para todos. Y es que, de la misma manera que los malos pueden hurtar nuestros datos, también pueden modificarlos. Esta tempestad que se avecina nos volverá vulnerables y sacudirá los cimientos de nuestra fe en un mundo que depende de los datos de modos que aún no somos completamente capaces de entender.

Capítulo 8

En la pantalla confiamos

> El mundo ya no está dominado por las armas, ni por la energía ni por el dinero. Está dominado por unos y ceros, por pequeños bits de datos. Todo está en los electrones. Ahí fuera se está librando una guerra, una guerra mundial. Pero ya no importa quién tiene más datos. Lo auténticamente relevante es quién controla la información: qué vemos, cómo trabajamos, qué pensamos. Lo importante es la información.
>
> *Cosmo* (BEN KINGSLEY), el malo en *Los fisgones*

Todos los sistemas efectúan comprobaciones. Las cinco mil centrifugadoras en funcionamiento en las instalaciones de enriquecimiento nuclear que Irán tiene en Natanz echaban humo y la República Islámica progresaba a buen ritmo en su programa de generación de energía nuclear «pacífica». Si las cosas continuaban su curso, pronto Irán tendría suficiente uranio 235 (U-235) enriquecido para crear su propia central nuclear o su primera bomba atómica, en función de a quién se preguntara. Aunque Irán siempre había insistido en que sus actividades nucleares eran exclusivamente para uso energético civil, gran parte del mundo, incluidos Estados Unidos, Europa, Israel y las Naciones Unidas, se mostraban menos convencidas de ello.

En 2005, la Organismo Internacional de Energía Atómica (OIEA) de la ONU determinó que Irán estaba incumpliendo el Tratado de No Proliferación Nuclear que había firmado y el organismo inspector transmitió sus preocupaciones al Consejo de Seguridad de la ONU[1]. En respuesta, la ONU exigió a Irán que suspendiera sus actividades de enriquecimiento nuclear en Natanz, exigencia a la que el presidente iraní a la sazón, Mahmud Ahmadineyad, respondió con un enfático «no». Los inspectores expertos de la OIEA concluyeron que Irán tenía conocimientos suficientes para diseñar y producir una bomba atómica operativa y la ONU impuso las consiguientes sanciones[2]. Pero ¿impedirían esas sanciones que Irán se hiciera con la bomba? Dada la prominencia del país en la lista de objetivos que Estados Unidos ha trazado en el «Eje del Mal», se precisaba alguna actuación adicional. Por motivos políticos, se descartó un ataque militar abierto, si bien un año después el presidente George W. Bush autorizó un ataque encubierto contra las instalaciones nucleares de Natanz y bautizó el programa de alto secreto con el nombre de Operación Juegos Olímpicos, según el *New York Times*[3]. El resultado fue «la manipulación encubierta más importante del espectro electromagnético desde la Segunda Guerra Mundial, cuando unos criptoanalistas descifraron el código Enigma

que permitió descodificar los códigos nazis»[4]. Los iraníes no eran un objetivo fácil y fueron lo bastante inteligentes como para no conectar la red de información más preciada de la República Islámica a Internet. Como consecuencia, los operativos asociados con la Operación Juegos Olímpicos no pudieron abrirse camino mediante una carretera poco protegida en la superautopista de la información. De ahí que fuera preciso montar y coreografiar con una precisión extrema a todo un entramado de agentes humanos, ingenieros y trabajadores de mantenimiento (espías y cómplices involuntarios por igual) para que el plan funcionara. ¿El arma elegida para llevar a cabo esta operación encubierta? Un pequeño llavero USB.

Para sabotear las centrifugadoras de Natanz se creó un nuevo tipo de ciberarma, capaz de salir del mundo virtual de los ordenadores e internarse en el mundo físico de los sistemas de control industrial. Me refiero a Stuxnet, un gusano informático sofisticadísimo que, según se cree, Estados Unidos e Israel crearon para mantener a su célebre enemigo a raya. Los creadores de Stuxnet copiaron el gusano en una sencilla unidad de USB y, una vez cargada y bloqueada, se dispusieron a buscar su cantera. Cómo logró entrarse de contrabando la unidad en Natanz y quién la insertó en la red informática de las instalaciones sigue siendo un misterio.

No obstante, lo que sí que se sabe es la rapidez con la que el *malware* se propagó por la infraestructura de TI de la central. La mera inserción de la unidad USB en el puerto USB de un ordenador infectó con una celeridad previamente no documentada el Microsoft Windows de la máquina aprovechando una vulnerabilidad del sistema operativo. Además, el gusano utilizaba un certificado de seguridad digital falsificado que indicaba que era de fiar y le permitió replicarse por toda la infraestructura TI de Natanz con total impunidad. A medida que se propagaba de escritorio en escritorio y de red en red, el virus formulaba una sencilla pregunta a cada máquina: ¿este ordenador está conectado a un sistema de control industrial fabricado por la empresa multinacional alemana Siemens?

Los estadounidenses y los israelíes habían hecho bien los deberes y sabían que las centrifugadoras de Natanz funcionaban con los controladores lógicos programables (CLP) industriales Siemens S7-417, que monitorizaban las válvulas y los sensores de presión de las centrifugadoras de la central. Si un ordenador no estaba conectado a un CLP de Siemens, el gusano no se replicaba y, sencillamente, moría. Si, en cambio, Stuxnet detectaba que un sistema informático de sobremesa o en red estaba conectado a un CLP Siemens, la ciberarma se ponía manos a la obra con tesón y se abría camino desde el ordenador Windows hasta el sistema de control industrial que gestionaba las centrifugadoras iraníes.

Los perpetradores del ataque sabían que refinar U-235 era una labor peliaguda. Las centrifugadoras IR-1 utilizadas en Natanz estaban diseñadas para girar a 100 000 rotaciones por minuto (RPM), un hito asombroso tanto en velocidad como en tecnología. Si las centrifugadoras giran demasiado lentamente, el U-235 necesario para generar energía nuclear (y bombas) no se separa de manera efectiva. Y si el

centrifugado es demasiado acelerado, las centrifugadoras vibran y se agitan de manera incontrolada hasta que la presión es tan fuerte que los motores se queman y hay que sustituirlas. Los creadores de Stuxnet sabían bien que sin centrifugadoras no había enriquecimiento y sin enriquecimiento no había bomba ni amenaza.

Los CLP de Siemens fueron claves para el ataque, pero los creadores de Stuxnet no eran cibercombatientes impetuosos movidos por una mentalidad de saquear y quemar. Perpetraron su ataque contra Natanz con paciencia, estrategia y astucia. En la primera fase del asalto a Natanz, Stuxnet se limitó a observar, sentado en silencio, mientras recopilaba de manera furtiva información para entender cómo funcionaban las centrifugadoras de enriquecimiento. El gusano grabó todos sus hallazgos en un movimiento planificado con maestría que demostraría ser crucial para el éxito de la operación.

Sin embargo, fue en la segunda fase cuando Stuxnet empezó a dar fe de sus verdaderas capacidades, a medida que el gusano fue haciéndose con el dominio de los sistemas de control industriales de Natanz. Poco a poco, sus dueños títere comenzaron a manipular las válvulas y los motores de las centrifugadoras responsables del enriquecimiento de U-235 en las instalaciones. Durante meses, años incluso, las centrifugadoras se aceleraron y ralentizaron, fluctuando de las especificaciones de 100 000 RPM para las que estaban diseñadas. La presión de las centrifugadoras aumentó, los rotores fallaron y la cantidad de uranio enriquecido conseguido empezó a mermar.

Entre tanto, en el interior de la sala de control de operaciones de alta seguridad de Natanz, todos los sistemas funcionaban a la perfección… al menos de acuerdo con las pantallas informáticas que monitorizaban los ingenieros de las instalaciones. Cada una de las miles de centrifugadoras estaba representada por una luz en una pantalla informática y se supervisaba con esmero para detectar posibles fallos en el funcionamiento del sistema. Una luz verde indicaba que la centrifugadora funcionaba correctamente, mientras que una luz gris o roja señalaba la existencia de problemas. Día tras día, los ingenieros observaron debidamente sus pantallas en busca de indicaciones de errores, pero las luces continuaban iluminadas en verde en los sistemas de seguridad de datos ante sus ojos. ¿Sistema de protección conectado en cascada? Verificado. ¿Presión de las centrifugadoras? Verificada. ¿Velocidad de los rotores? Verificada. Tanto las pantallas en las paredes como las pantallas de sus escritorios y las pantallas de los paneles de control, todos los sistemas en el interior del centro de mando de operaciones indicaban a los iraníes que sus ambiciones nucleares iban sobre ruedas. Nada más lejos de la realidad.

El gusano Stuxnet se diseñó para que, en un primer momento, causara un daño contenido. Poco a poco, algunas centrifugadoras aceleraron el ritmo de centrifugación hasta quedar fuera de control, pero los iraníes culparon de ello a piezas defectuosas o a la incompetencia de sus ingenieros. Cada centrifugadora parecía fallar por un motivo distinto: una iba demasiado lenta, la otra demasiado rápida, otra parecía haber

estado sometida a demasiada presión… La calidad del uranio procesado mermaba y era inutilizable. Se llevaron a cabo inspecciones sucesivas de las instalaciones y los investigadores continuaron observando atentamente el estado del conjunto de la operación desde los ordenadores de la sala de control. A medida que transcurría el tiempo, docenas y luego centenares de centrifugadoras empezaron a fallar. Las ambiciones nucleares de Irán comenzaban a estar en entredicho. ¿Qué diantre estaba sucediendo? Resultó que los iraníes habían depositado demasiada confianza en las pantallas informáticas que gobernaban su valiosísima instalación de enriquecimiento nuclear hermética.

Los registros de datos y las grabaciones computacionales de los sistemas de control industrial perpetrados con sigilo por el gusano Stuxnet en la primera fase del ataque tenían un objetivo claro, pese a que no fuera inmediatamente obvio: documentar en detalle qué aspecto tenían los CLP de Siemens cuando funcionaban en plenas capacidades. Al dejar que los rotores girasen según lo previsto y que la presión se situara en niveles esperados, todos los sistemas seguían funcionando con luz verde. Stuxnet capturó todos estos datos y los grabó en el equivalente CLP de un VCR, cuidadosamente guardados para la posteridad. Lo que sucedió a continuación parece sacado de una película supertaquillera de Hollywood, retratado multitud de veces en filmes como *Ocean's Eleven* o *La búsqueda*. Los atacantes se limitaron a pregrabar vídeo de la actividad del casino o de la sala de seguridad contra la que iba a perpetrarse el ataque y lo reprodujeron en las pantallas de los observadores y el personal de seguridad.

Mientras las centrifugadoras de enriquecimiento de uranio se aceleraban hasta perder el control en Natanz, Stuxnet interceptó magistralmente los valores de entrada reales de los sensores de vibración, presión y rotación antes de que llegaran a la sala de control operativa supervisada por los ingenieros de la central. Y en lugar de presentar los datos correctos en tiempo real enviados por las CLP de Siemens, Stuxnet se limitó a sustituirlos por la información pregrabada que había acumulado durante la fase inicial de la operación, y por eso los sistemas parecían funcionar a la perfección. Aquel movimiento brillante implicó que, aunque en realidad los sistemas de control industriales estaban fundiéndose y pedían digitalmente socorro a gritos, las señales de advertencia rojas emitidas mediante luces interminentes por el sistema fueron suplantadas por un mar de sosiego verde en los monitores de los iraníes que controlaban Natanz. Cuando las centrifugadoras quedaron fuera de control y se desmembraron, los operadores humanos de la sala de control digital no imaginaban que un gusano informático con un nombre gracioso enviado en una misión de búsqueda y destrucción había pirateado y secuestrado su realidad.

La vida en un mundo mediado

Por desgracia, tienes mucho más en común con los iraníes de lo que imaginas. Aunque seguramente no te dediques a producir U-235, también dependes de las pantallas en tu vida cotidiana para traducir el mundo que te rodea. Tu teléfono móvil te dice quién te ha llamado, tu ordenador te recuerda que tienes que actualizar el sistema operativo y el GPS de tu coche te indica cómo llegar hasta la reunión de esta mañana. Todo esto y más ocurre antes de que te acabes la segunda taza de café. ¿El resultado de ello? Hemos dejado de guiarnos por nuestras capacidades sensoriales humanas principales e innatas para vivir la vida y, en su lugar, la experimentamos mediante pantallas, muros virtuales que nos apartan de nuestros sentidos intrínsecos y definen el mundo que nos rodea. Las pantallas se interponen entre nosotros y el mundo real, proyectando información que supuestamente equivale a la realidad, pero que, a lo sumo, sólo es una burda aproximación a ésta y, además, puede manipularse fácilmente.

En nuestros aeropuertos, hospitales, bancos y cajeros automáticos, las pantallas se han convertido en un elemento omnipresente. Pero las pantallas de hoy en día son «tontas», en el sentido de que se limitan a presentar la información subyacente contenida en sistemas de datos, sistemas a todas luces vulnerables. Quienes controlan el código informático también controlan las pantallas y, por ende, nuestras vivencias y percepciones. Todo, desde los videojuegos hasta las urnas electrónicas, puede falsificarse, y en este mundo nuevo en el que vivimos, el hecho de ver algo con los propios ojos y oírlo con los propios oídos no es en absoluto garantía de que sea legítimo, correcto o seguro: las pantallas que miramos pueden engañarnos de modos que aún no alcanzamos a comprender.

Tanto si eres consciente de ello como si no, toda tu experiencia en el mundo online visualizada en pantallas digitales está siendo conservada. Parte de esa filtración, por descontado, es positiva. Con miles de millones de tuits, mensajes de Snapchat, actualizaciones de estado y publicaciones en blogs, es imposible digerir el volumen de datos que se pone en circulación a diario. Conscientes de ello, las empresas de Internet dedican todo su empeño a saber qué te gusta y personalizar tu experiencia virtual aplicando una serie de algoritmos informáticos. Facebook estudia tus enlaces a sitios web, imágenes, toques, mensajes, eventos y «Me gusta» para personalizar lo que ves en la pantalla cada día. Como resultado de ello, no ves la mayoría de las cosas que publican tus amigos o que se postean en las páginas que sigues, y tus amigos ven en torno a un diez por ciento de tus actualizaciones en sus resúmenes de noticias[5]. Por mucho esfuerzo que Facebook ponga en estudiarte y segmentarte para sus anunciantes, resulta casi igual de arduo determinar cuál de las publicaciones de tus amigos te gustaría ver cada vez que visitas su sitio web o lanzas su aplicación[6]. Ahora bien, ¿por qué lo hace? Simple y llanamente, porque Facebook, Google y otras empresas de Internet saben que si te proporcionan el material «correcto», pasarás más tiempo en sus sitios web, seleccionarás más enlaces web y ello les permitirá presentarte cada vez más anuncios.

Desde luego, Facebook no es la única empresa en este juego. Google también cuantifica todas tus búsquedas previas y, lo que es más importante, los enlaces que has activado, con el fin de personalizar tu experiencia virtual. En su libro *The Filter Bubble*, el investigador en materia de tecnologías Eli Pariser documentaba de manera pormenorizada este fenómeno. Brindarte los resultados «correctos» es un gran negocio, motivo por el cual se dedican millones de algoritmos informáticos a esta labor. Según consta, Google tiene al menos cincuenta y siete señales distintas de personalización que rastrea y analiza antes de responder a tus preguntas, supuestamente con el fin de incorporar el tipo de ordenador que usas, el navegador que tienes abierto, la hora del día, la resolución de tu monitor, los mensajes que has recibido en el Gmail, los vídeos que has visionado en YouTube y tu localización física[7]. Google altera en tiempo real los resultados de búsqueda que te muestra en función de lo que sabe acerca de ti. Una búsqueda por la palabra «aborto» devuelve enlaces de «planificación familiar» a unas personas y vínculos a «Catholic.com» a otras; si formulas una pregunta sobre «Egipto», es posible que tú recibas resultados acerca de la Primavera Árabe, mientras que a tu madre se le muestre información sobre las pirámides o cruceros por el Nilo. Al igual que hizo Pariser, puedes realizar este experimento tú mismo y los resultados te proporcionarán una perspectiva iluminadora de cómo te ve Google.

El meollo de la cuestión es que no existe un «Google estándar». Eric Schmidt ha admitido públicamente que «resultaría muy difícil a un usuario ver o consumir algo [online] que no se haya personalizado para su perfil»[8]. Si bien esto no tiene por qué considerarse malo obligatoriamente, sí cabe formularse algunos interrogantes importantes con respecto a cómo otras personas, al parecer en nuestro beneficio, seleccionan, clasifican y conservan toda esta información. Ahora bien, el desafío principal estriba en que ni Google, ni Facebook, ni Netflix ni Amazon hacen públicos sus algoritmos. De hecho, los métodos que aplican para filtrar la información que ves están protegidos por estrictos derechos de propiedad y son la «salsa secreta» que brinda tantos beneficios a cada una de estas empresas. El problema de este procesamiento de la información mediante una «caja negra» de algoritmos invisibles es que no sabemos qué se modifica para nosotros y qué *no* vemos. Por consiguiente, nuestras vidas digitales, mediadas por un mar de pantallas, están siendo manipuladas de forma activa y filtradas a diario de modos a la par opacos e indescifrables. Este viraje fundamental en la manera como la información fluye por Internet no sólo moldea cómo nos informamos sino cómo percibimos el mundo. La mayoría de nosotros vivimos en burbujas filtradas… y ni siquiera somos conscientes de ello.

Alrededor del planeta, los países deciden cada vez más a qué deben tener acceso los ciudadanos y qué información debería prohibirse. Con argumentos persuasivos como «proteger la seguridad nacional», «garantizar los derechos de propiedad intelectual», «preservar los valores religiosos» y, el favorito de todos los tiempos, «proteger a los niños», los gobiernos amplían cada vez más sus cortafuegos

nacionales con el objetivo de censurar Internet[9]. Algunas de estas técnicas de filtrado se desvelan al público general. Por ejemplo, en Francia y Alemania, los sitios que promueven el nazismo y niegan el Holocausto se clausuran de manera abierta. En Siria, YouTube, Facebook, Amazon, Hotmail y los sitios web prokurdos se han bloqueado. En Arabia Saudí, 400 000 sitios web se han restringido, incluidos aquellos que analizan temas políticos, religiosos o sociales incompatibles con el islam o con las creencias personales del soberano[10]. Sin embargo, en muchos casos no recibes ninguna indicación de que tu información online esté siendo censurada; en su lugar, el contenido sencillamente no aparece. En los Emiratos Árabes Unidos, el gobierno ha bloqueado todo acceso al dominio .il, de Israel, borrando con ello la existencia del Estado judío en el mundo virtual.

Empresas tecnológicas han colaborado en programas de censura nacional y han accedido a las demandas estatales de filtrar contenido ofensivo en tiempo real, como hizo Google al abrirse al mercado chino en 2005. Quizá el gobierno más versado y riguroso en sus programas de filtrado de Internet sea China. La «Gran Muralla Cortafuegos» de China garantiza que sus miles de millones de habitantes sean incapaces de consultar temas políticos comprometidos, como las manifestaciones en la plaza de Tiananmén, detalles vergonzantes acerca de los dirigentes del país, o debates sobre los derechos de los tibetanos, el Dalai Lama, Falun Gong, la independencia de Taiwán, la reforma política o los derechos humanos. Ahora bien, la censura en Internet no sólo la practican los regímenes autocráticos o déspotas. En 2014, más de cuatro mil millones de personas habitaban en países que practican alguna suerte de filtrado de Internet.

Las pantallas no te muestran lo que pasa realmente en el mundo, sino lo que el gobierno o Facebook creen que deberías ver. Si buscas algo y no lo encuentras, ¿cómo puedes saber de su existencia? Para parafrasear una antigua pregunta filosófica: si un árbol cae en Internet y ningún motor de búsqueda lo indexa, ¿emite algún ruido? En nuestras vidas cada vez más mediadas por pantallas, cuando algo no existe en Internet, sencillamente no existe. Si un evento no aparece listado en Google, no ha sucedido. Aunque es posible que sí aparezca en Google y aún no haya ocurrido. Bienvenido al mundo de los ardides digitales, una sala de los espejos virtual representada en pantallas en la que todo es posible por arte de magia.

El hondo riesgo de vivir en un mundo mediado por la tecnología es que crea oportunidades gigantescas para que la información se manipule de modos indetectables que ninguno de nosotros prevemos ni entendemos. Hay pantallas por doquier, y emiten pitidos, sonidos o parpadeos para llamar nuestra atención. Pero ¿qué sucede si esas pantallas mienten? ¿Si nos aportan información falsa y nos engañan? En el mundo actual, todo lo que vemos en las pantallas puede falsearse y parodiarse fácilmente. Pregúntale a cualquiera que haya visitado alguna vez una web de citas en Internet y te lo confirmará: lo que ves no es siempre lo que obtienes.

No cuenta

> ¡Como que a veces llegué hasta a creer en seis cosas imposibles antes del desayuno!
>
> LEWIS CARROLL, *A través del espejo*

¿Qué tienen en común los piratas informáticos, los estafadores y la delincuencia organizada con Facebook, Google y la NSA? Pues que cada uno de ellos es perfectamente capaz de mediar y controlar la información que aparece en la pantalla de tu ordenador. En un mundo donde la información es poder, quienes controlan el flujo de datos que llega a tus pantallas también controlan otras cosas. Topamos con este comportamiento a diario, cada vez que nos conectamos a Internet. Muchos de nosotros no nos plantearíamos efectuar una compra importante o reservar una mesa en un restaurante nuevo para una ocasión especial sin primero consultarlo en Internet. ¿Quién mejor para informarnos que otros clientes y comensales? Prácticamente el 90 por ciento de los consumidores corroboran que las reseñas en Internet influyen en sus decisiones de compra, y un estudio de Nielsen detectó que un asombroso 70 por ciento confían tanto en las reseñas que leen online como en las recomendaciones de sus amigos[11]. Por desgracia, de acuerdo con una investigación llevada a cabo por el fiscal general del estado de Nueva York, el 25 por ciento de las reseñas en Yelp, uno de los sitios web más populares de este tipo, son espurias[12]. Peor aún, en septiembre de 2014, un tribunal de apelaciones federal consideró completamente legal que Yelp manipulara sus puntuaciones en función de qué empresas se anunciaran en su sitio web; de este modo, los inversores más potentes podían obtener legalmente cinco estrellas, incluso aunque los usuarios les asignaran sólo una[13]. Las reseñas en eBay, Amazon y TripAdvisor también se falsifican con facilidad, y muchas de esas publicaciones con cinco estrellas que ves las escriben las propias empresas o intermediarios a sueldo. Incluso existen empresas cuyo modelo de negocio integral consiste en falsificar el sistema de reseñas en Internet. Esta práctica se conoce con el nombre de «*astroturfing*» («intoxicación»)[*] y es generalizada. Una empresa investigada por el estado de Nueva York, conocida como Zamdel Inc., fue acusada de redactar más de quince mil reseñas falsas en Yelp y Google Places[14]..

Pensaba que eras mi amigo

De acuerdo con el informe anual de 2014 del propio Facebook, en torno al 11,2 por ciento de sus cuentas son falsas. Teniendo en cuenta que la empresa de redes sociales más importante del mundo tiene mil trescientos millones de usuarios, eso representa

que unos 140 millones de cuentas de Facebook son fraudulentas y que dichos usuarios sencillamente no existen[15]. Con 140 millones de habitantes, Facebooklandia sería el décimo país más poblado del mundo. Tal como las puntuaciones de Nielsen en los televisores determinan distintas franjas de precios por publicidad para *The Walking Dead* y la Super Bowl, las ventas de anuncios en Internet se deciden por cuántos ojos puede atraer un sitio web o una red social…, si es que tales datos son creíbles.

¿Quiere tener 4000 seguidores en Twitter? Puedes comprarlos por cinco dólares[16]. ¿Quieres 100 000 fans en Facebook? Ningún problema: SocialMediaCorp.org te los vende por sólo 1500 dólares[17]. ¿Tienes más presupuesto para invertir? ¿Qué te parece entonces hacerte con un millón de amigos nuevos en Instagram? «Te hacemos un precio especial por ser tú», sólo 3700 dólares. Tanto si lo que buscas son favoritos, «Me gusta», retuits, votaciones o visualizaciones de página, todo está a la venta en sitios web como Swenzy, Fiverr y Craigslist. Estas cuentas de redes sociales fraudulentas se utilizan para promocionar falsamente un producto, servicio o empresa, por supuesto por un pequeño precio. Tales labores se llevan a cabo, en su inmensa mayoría, en el mundo en desarrollo, en lugares como India y Bangladesh, donde seres humanos de carne y hueso gestionan las cuentas. En otros puntos del planeta, como Rusia, Ucrania y Rumanía, robots informáticos controlan íntegramente este proceso mediante *scripts*, pequeños programas que implementan las instrucciones automatizadas precodificadas que se les asignan, como «haz clic en el botón “Me gusta”» una y otra vez utilizando identidades falsas.

De la misma manera que los seres mitológicos que se metamorfoseaban eran capaces de transformarse físicamente de un ser en otro, estos metamorfoseadores de pantallas modernos despliegan sus propios poderes mágicos, y los delincuentes se mueren de ganas de llevarse una porción del pastel, para lo cual estudian sus técnicas y las despliegan contra dianas fáciles con vistas a obtener beneficios ingentes. De hecho, muchos de estos clics se realizan para cometer «fraude de clics». Las empresas pagan a otras empresas como Facebook y Google cada vez que un cliente potencial hace clic en uno de los anuncios o enlaces que aparecen en Internet, pero las mafias organizadas han averiguado cómo vulnerar el sistema para canalizar los beneficios en su dirección mediante las llamadas redes publicitarias, que obtienen capital de todos esos clics adicionales. Espoleadas por las críticas, las empresas de redes sociales han intentado recortar el número de perfiles falsos que existen. Los resultados de las actuaciones de Facebook fueron reveladores. Rihanna y Shakira perdieron 22 000 fans en Facebook, Lady Gaga vio cómo 32 000 de los suyos desaparecían, y *Texas Hold’Em Poker* de Zynga contaba con 100 000 supuestos seguidores que se desvanecieron en el aire[18].

Si Facebook tiene 140 millones de perfiles falsos, es imposible que se hayan creado manualmente uno a uno; tiene que haber algo mucho más siniestro en marcha, como en efecto ocurre. Esta práctica de creación de reseñas e identidades falsas se

denomina *sock puppetry* (literalmente «marionetas de calcetín») en referencia a las marionetas infantiles que se crean introduciendo una mano en un calcetín para darle vida. En el mundo virtual, la delincuencia organizada crea identidades falsas combinando *scripts* informáticos. La automatización web y las redes sociales generan un sinnúmero de identidades virtuales. Es una estrategia sencilla y lo bastante barata como para permitir a aquéllos con intenciones falaces dar vida a centenares de miles de ciudadanos virtuales falsos.

Basta con consultar un directorio de los nombres más comunes en un país o una región concretos disponible en Internet para el público general. Se configura el *bot* de los *scripts* para que se limite a seleccionar un nombre y un apellido, elija una fecha de nacimiento y configure una cuenta de correo electrónico gratuita. A continuación, se rastrean sitios de fotografía en línea, como Picasa, Instagram, Facebook, Google y Flickr para elegir una imagen adecuada a la edad de la identidad falsa. Dotado con una dirección de correo electrónico, un nombre, una fecha de nacimiento y una fotografía, simplemente tienes que configurar una cuenta en Facebook, Twitter o Instagram. Como paso final, enseñas a tus identidades falsas a hablar mediante *scripts* para que salgan al mundo y envíen solicitudes de amistad, reposteen los tuits de otras personas y den al «Me gusta» de manera aleatoria en cosas que ven online. Tus *bots* incluso pueden comunicarse y cruzar publicaciones entre sí. En un abrir y cerrar de ojos, tendrás miles de identidades falsas a tu disposición para que las utilices como te convenga. Son estos ejércitos de «marionetas» lo que los delincuentes utilizan como elementos clave para perpetrar sus ataques de *phishing*, para que escriban reseñas falsas en Internet, para que engatusen a los internautas para descargarse *software* espía y para que cometan un amplio abanico de fraudes económicos… todos ellos fundamentados en el hecho de equivocarnos en quién o qué ponemos nuestra confianza.

Error fatal del sistema

Vivimos en un mundo regido por el lema «en la pantalla confiamos». Buscamos asesoramiento y consejos en los ordenadores de manera prioritaria. Dependemos de las pantallas para que nos den respuestas y rara vez nos cuestionamos los resultados. Sin embargo, si tu programación es pobre o tus datos principales son incorrectos, estos errores se reflejarán en los resultados que recibas. El conocido dicho GIGO (del inglés «Garbage In, Garbage Out» o «si entran datos erróneos, saldrán datos erróneos») es uno de los axiomas de la ciencia computacional. En el pasado, nuestra confianza limitada en la tecnología nos aislaba y protegía de cometer muchos de estos errores. Sin embargo, en la era de los datos masivos, el cálculo ha cambiado… y lo ha hecho a lo grande. A todos nos afectan los errores de las bases de datos de un modo u

otro y las implicaciones de estas imprecisiones aumentan día tras día. De acuerdo con la Comisión Federal de Comercio, en torno al 25 por ciento de los historiales crediticios de los consumidores contienen errores y los agentes intermediarios de datos, como Acxiom, han admitido que el 30 por ciento de los datos que conservan sobre nosotros podrían ser imprecisos[19].

Cuando entre cuarenta y cincuenta millones de estadounidenses afectados por estos errores intentan alquilar un apartamento, comprar un coche, contratar una hipoteca o solicitar un empleo, descubren que el error de otra persona se ha convertido en su pesadilla. Si «de acuerdo con nuestro ordenador» supones un riesgo para la concesión de un crédito, no hay «si», «y» o «peros» que valgan. En la actualidad, a diario se adoptan millones de decisiones con datos erróneos, incompletos o imprecisos, a menudo sin ninguna verificación adicional. Si el problema se limitara a los historiales crediticios, podría ser tolerable… con cierto esfuerzo. Sin embargo, la vida regida por este «en la pantalla confiamos» conlleva que los errores informáticos no sólo afectan a nuestras economías, sino que también pueden afectar a nuestra vida personal y a nuestra libertad.

Mientras el mundo de la medicina da grandes pasos por digitalizar los historiales de los pacientes en un esfuerzo por ahorrar dinero, mejorar la eficacia y entender mejor las enfermedades a partir de estos datos masivos, ello ha tenido un coste imprevisto: la precisión. Decenas de millones de registros médicos electrónicos contienen información incorrecta acerca de los pacientes y los datos erróneos en las pantallas informáticas pueden matar, literalmente[20]. Gary Foster, un joven de veintisiete años de Essex, Inglaterra, falleció en el University College Hospital de Londres cuando un fallo técnico en el sistema informático de las instalaciones hizo que se le suministrara una sobredosis de su medicación para el cáncer durante su hospitalización. El personal hospitalario, siguiendo una receta introducida de manera imprecisa, le suministró una dosis letal de quimioterapia para el tratamiento de su cáncer testicular[21]. Es más, depositar una fe excesiva en las pantallas informáticas no sólo puede matar, sino que además puede tener un impacto perjudicial en la seguridad pública.

En California, un fallo informático provocó la puesta en libertad de 450 delincuentes peligrosos cuando un error en el sistema indicó al personal penitenciario que liberara a algunos de los delincuentes más violentos del estado[22]. Miembros de bandas callejeras, violadores, ladrones armados y convictos clasificados como con un «alto riesgo de violencia» salieron de prisiones de todo el estado porque los funcionarios consideraron fidedigna la información que aparecía en sus pantallas. Por supuesto, los errores en la justicia criminal son frecuentes, y no sólo ponen en libertad a culpables, sino que también inculpan a inocentes. En Gran Bretaña, agentes policiales de la Oficina de Registros Criminales nacional admitieron que más de veinte mil personas habían sido consideradas erróneamente como delincuentes debido a errores en los datos contenidos en su sistema[23]. Aquella metedura de pata masiva

implicó que se abriera expediente delictivo a miles de personas inocentes por delitos que no habían cometido. «Agente, se lo aseguro, se equivoca de persona» es una frase que los policías están acostumbrados a escuchar; por desgracia para los involucrados en aquel episodio, lo que dice la pantalla es la verdad, hasta que se demuestre lo contrario. En todo el Reino Unido, víctimas de estos errores vieron cómo les denegaban empleos y puestos de voluntariado y cómo sus reputaciones quedaban arruinadas, todo a causa de nuestra fe inquebrantable en las pantallas.

En la actualidad afrontamos una confluencia de fenómenos, tanto humanos como técnicos, que se condensan como una tormenta perfecta para plantear peligros de lo más peliagudos para la sociedad. Con cada generación sucesiva, nos volvemos más cómodos, aunque sea de manera inconsciente, y nos limitamos a seguir a ciegas las indicaciones que nos dan las máquinas. El lema «si entran datos erróneos, saldrán datos erróneos» ha sido suplantado por «si entran datos erróneos, saldrá la verdad absoluta»: si lo dice el ordenador, tiene que ser verdad. El problema de este razonamiento es que, en tanto que sociedad, confiamos de continuo en datos incorrectos, un problema enconado que acabará volviéndose en nuestra contra. Las burbujas de filtros, la censura invisible en los motores de búsqueda, los cortafuegos nacionales y los datos equivocados implican que tenemos un problema de integridad fundamental en el modo de percibir el mundo o, para ser más preciso, en el modo como nos presentan el mundo por medio de nuestras pantallas.

Cuando ver no es creer

En los capítulos anteriores nos hemos concentrado ampliamente en lo que ocurre cuando tus datos se filtran y la confidencialidad de tu información se vulnera. Sin duda, los delincuentes aprovechan cualquier oportunidad que se les presenta al robar tus datos. No obstante, existe una amenaza mucho más profunda e insidiosa para el mundo de la información, que es la modificación de los datos. Cada vez son más los delincuentes, *hackers*, terroristas y gobiernos que se infiltran en sistemas de datos, no ya para robar información, sino para manipular subrepticiamente la manera en que aparece en nuestras pantallas, tal como hemos visto que sucedió en Natanz. Por tanto, la integridad misma de la información mundial es objeto de ataque. De forma lenta e imperceptible y con suma precisión, los atacantes pueden introducirse en nuestros sistemas de datos y modificar de manera encubierta toda la información subyacente. Cuando se produce un ataque informático, es mejor que nos roben la información que no que la modifiquen sin nuestro conocimiento.

En el largometraje de 1995 *La red*, Sandra Bullock interpreta a una retraída analista de sistemas que accidentalmente descubre una trama de una organización ciberterrorista diabólica dispuesta a apoderarse de los sistemas de información

mundiales. La película abre con el subsecretario de Defensa de Estados Unidos suicidándose después de saber que ha dado positivo en VIH en el Bethesda Naval Hospital. Luego se demuestra que el político no tenía el VIH, sino que unos piratas informáticos habían modificado los resultados de sus análisis médicos en represalia por su persecución de ciberdelincuentes a escala internacional, resultados que, cumpliendo con su deber y basándose en los datos que aparecían en la pantalla de su ordenador, el médico le comunicó. La vergüenza de ser seropositivo pesó demasiado al subsecretario conservador y precipitó su suicidio.

Vivimos en un mundo de guerra informativa, en el que la desinformación informática diseminada mediante una serie de pantallas parpadeantes tiene repercusiones en el mundo real. Los acontecimientos narrados en esta película son plausibles hoy en día. En todo el mundo se han pirateado sistemas de datos policiales, inclusive en Australia, Inglaterra, Italia, Memphis, Montreal, Hong Kong y Honolulu[24]. En 2013, se vulneró el registro de permisos de conducir nacionales de la policía danesa y se cree que los *hackers* efectuaron cambios en los sistemas de datos de las autoridades policiales subyacentes[25]. También en 2013, pero en Filadelfia, una base de datos de testigos de algunos de los delitos más notorios de la ciudad fue saboteada por una banda delictiva local. En consecuencia, los nombres, las direcciones y las fotografías de docenas de testigos protegidos se publicaron en Instagram con el eslogan «Soplones a la vista». Muchas de las personas cuyas identidades se revelaron habían testificado en vistas ante un gran jurado secreto y, al cabo de pocos días, el usuario de la cuenta en Instagram, conocido como rats215, contaba ya con ocho mil seguidores. Un testigo de diecinueve años en un caso de homicidio fue tiroteado a modo de represalia. En lo que acabó convirtiéndose en una intimidación de los testigos a gran escala, numerosos visitantes de la red social postearon comentarios como «exterminad a los soplones» o «metedles un balazo»[26].

En Massachusetts, un reo que cumplía condena por pirateo informático recibió permiso para acceder al ordenador de la biblioteca de la prisión con el fin de efectuar búsquedas legales sobre su propio caso. Una vez puso los dedos en el teclado, fue capaz de abrirse camino a través de la red informática del Departamento de Corrección y obtener acceso a los expedientes de otros presos, además de a los nombres, fechas de nacimiento, números de la Seguridad Social, direcciones de sus hogares y números telefónicos de los mil cien guardas de la prisión[27]. A tenor de la escasa seguridad de los sistemas de justicia criminal cabe preguntarse cuántos convictos más se han liberado por error, como aquellos 400 presos peligrosos de California, porque los datos subyacentes se han falsificado y modificado de manera voluntaria. La respuesta es que no lo sabemos, ya que los funcionarios gubernamentales detestan hablar de este tema.

Ahora bien, por abiertos y vulnerables que sean los ordenadores de los cuerpos de seguridad, son un auténtico Fort Knox en comparación con nuestros historiales médicos electrónicos[28]. Olvida por el momento los millones de errores accidentales

indicados previamente; el Departamento de Salud y Servicios Sociales de Estados Unidos (HHS) ha determinado que, desde 2009, se ha accedido sin autorización al menos a los historiales médicos electrónicos de veintiún millones de estadounidenses[29]. De hecho, el HHS ha documentado más de novecientas vulneraciones de este tipo en hospitales de todo el país[30]. Pero ¿de cuántas no se ha informado? La ley federal sólo obliga a comunicar estas vulneraciones si el ataque se perpetra contra más de quinientos historiales. Los delincuentes organizados apuntan a datos médicos de modos muy variopintos, que engloban desde el fraude a Medicare hasta la extorsión. En Virginia, unos piratas informáticos accedieron a ocho millones de historiales de pacientes y a treinta y cinco millones de recetas mantenidas por el Departamento de Salud del estado y amenazaron con publicar la información a menos que Virginia pagara un rescate de diez millones de dólares. En todo el mundo, los sistemas de datos médicos electrónicos son muy porosos y las personas malintencionadas son perfectamente capaces de utilizar esos datos con consecuencias letales.

Una y otra vez, médicos, enfermeras y técnicos seguirán las indicaciones que se les presenten en las pantallas de sus ordenadores, incluso cuando la información sea incorrecta, tal como hemos visto al relatar el error del sistema hospitalario que provocó la muerte a Gary Foster. Si la pantalla dice que eres seropositivo, el hospital te lo comunicará. O lo que es peor aún, si tu tipo sanguíneo aparece como O positivo y un *hacker*, enemigo o adversario modifica la base de datos del hospital y lo convierte en A negativo antes de que te sometan a una operación quirúrgica, es más que probable que no salgas vivo de ella[31]. Y lo mismo sucedería si alguien borrara maliciosamente tu alergia a la penicilina de tu gráfico digital y una enfermera cumpliera una orden médica que le indicara que inyectara quinientos miligramos de ese medicamento en tu vía intravenosa.

La hondas consecuencias de esta mentalidad de «en la pantalla confiamos» pueden abrir la puerta a todo un abanico de delitos nuevos, incluidos métodos novedosos de cometer homicidios. En repuesta a ello, los delincuentes han concebido un amplio espectro de metodologías para aprovecharse de un mundo que ha subsumido la inteligencia humana a la digital y la virtual. Seres viles están demostrando ser expertos en los llamados ataques con intermediario, consistentes en insertarse entre la realidad y los datos que aparecen en nuestras pantallas. ¿El resultado? Una guerra sin cuartel contra la integridad de la información que apilamos a causa de la revolución de los datos masivos.

La pantalla del delito

Los delincuentes han urdido un plan de ataque contra cada pantalla de tu vida. Uno de los timos más habituales en Internet es el fenómeno del *phishing*, técnica consistente en que los estafadores se hacen pasar por un sitio web legítimo con el fin de adquirir información como contraseñas y números de tarjetas de crédito. El término «*phishing*» es una alteración gráfica de *fishing* («pescar») que emplean los *hackers*, ya que esta técnica consiste en intentar que un pez inocente muerda el anzuelo de un enlace malicioso y pique. La delincuencia organizada que lleva a cabo estafas de *phishing* intenta engañar a los internautas para que hagan clic en un enlace que los conduce a un sitio web fraudulento controlado por estafadores. Recibimos mensajes de *phishing* en los buzones de entrada de nuestro correo electrónico, vía SMS, tuits, mensajes instantáneos y actualizaciones de estado de Facebook. Supuestamente los envían nuestros bancos, empresas de televisión por cable, planes de jubilación, redes sociales y operadoras de telefonía móvil, y van dirigidos a usuarios de todo el mundo, si bien el mayor número de víctimas se concentra en Estados Unidos, el Reino Unido y Alemania[32].

En última instancia, todos los ataques de *phishing* dependen de que un usuario ingenuo haga clic en un enlace o archivo adjunto a un mensaje que o bien lo conducirá a un sitio web falso o bien instalará *software* malicioso en su máquina. Los delincuentes aprovechan enlaces de hipertexto HTML para incrustar sus ataques en el código informático oculto. Los mensajes de *phishing* adoptan la forma de tarjetas electrónicas falsas, mensajes de correo electrónico enviados desde nuestro banco, ofertas de empleo, descuentos u ofertas demasiado buenas para ser verdad en las redes sociales. Estos comunicados maliciosos, repletos de errores gramaticales y ortográficos en años pasados, se han ido profesionalizando cada vez más y hoy en día son casi indiferenciables de sus homólogos fidedignos. Los delincuentes saben exactamente cómo subvertir la confianza que has depositado en la pantalla imitando visualmente los sitios web que fingen ser y confundiendo tus sentidos con trucos de prestidigitación.

Lo más típico es que te llegue un mensaje de una dirección como seguridad@bancodeespaña.com informándote de que debes actualizar tu perfil o de que han cancelado tu cuenta debido a una actividad sospechosa. «¡Caramba! Parece importante, será mejor que le eche un vistazo», piensas. Lo que desconoces es que la dirección de correo electrónico que aparece en tu buzón de entrada es ridículamente fácil de imitar o falsificar. Cada vez que configuras una cuenta nueva de correo electrónico en cualquier programa informático de *email* como Outlook, Mac *Mail* o Thunderbird, se te solicita que introduzcas un nombre y una dirección de correo electrónico. Si un estafador escribe «Equipo de Seguridad del Banco de España» como su nombre en el programa de correo electrónico, eso será lo que aparecerá en tu buzón de entrada. Así de sencillo. Sólo examinando las cabeceras del mensaje podrías darte cuenta de que la dirección de correo electrónico que han utilizado los malos en realidad era notificaciones@seguridadbancodeespaña.com…, pese a ello

demasiado «creíble» como para despertar sospechas en el internauta medio.

En todos los sentidos, el mensaje parece proceder de tu banco (usa la misma tipografía, la misma paleta de colores, el mismo logotipo)…, pero no es así. Aunque en el enlace invisible se lea www.bancodeespaña.com, en su lugar te conducirá al sitio web www.banc0deespaña.com (un 0 en lugar de *o*) o incluso a bancodeespaña.actualizaciondecuentas.com (donde actualizaciondecuentas.com es el dominio real que estás visitando, propiedad de los delincuentes, mientras que Banco de España es una carpeta que albergan en su sitio web para engañarte); en la misma línea, www.citibank.com será suplantado por www.citiibank.com (dos íes en la dirección falsa; casi nadie se daría cuenta). Los mensajes de *phishing* indican de manera sutil qué quieren de ti mediante un enlace incrustado que contiene una poción venenosa imposible de pasar por alto, escrita en un tipo de letra grande y con un gran botón de color: «Para actualizar los ajustes de seguridad y proteger su cuenta, haga clic aquí». Y entonces ya eres suyo.

Ese clic fatídico te conducirá al sitio web de Citiibank.com, donde se te solicitará que inicies sesión y proporciones tus credenciales y, cuando lo hagas, los ladrones registrarán tu nombre de usuario y contraseña, además de otra información personal. Y entonces será cuando se pondrán manos a la obra de verdad. El *phishing* es un delito umbral, un primer paso que suministra a los ladrones los datos que precisan para perpetrar la segunda fase de su plan contra ti, que puede abarcar desde suplantación de identidad hasta fraude financiero, fraude fiscal o fraude a las aseguradoras. De la misma manera que los ingenieros de Natanz contemplaban en sus pantallas una realidad convincente pese a ser ficticia, también a ti te acorralarán los delincuentes, que llamarán a tu puerta cada día desplegando técnicas de engaño similares.

Para los delincuentes, los costes de poner en funcionamiento estas farsas digitales son ridículamente exiguos. En el mercado digital clandestino se venden kits de *phishing* completamente automatizados capaces de enviar mensajes fraudulentos a 500 000 direcciones de correo electrónico por sólo sesenta y cinco dólares y, tal como se ha mencionado con anterioridad, los delincuentes aprovechan la ventaja de las cuentas creadas con identidades falsas para ampliar su alcance[33]. De ahí que lleguen a nuestros buzones de entrada más de cien millones de mensajes de *phishing* cada día[34]. Según un estudio sobre la economía de estos ataques realizado por Cisco, unas ocho personas de cada millón caen en la trampa, con unas pérdidas medias de dos mil dólares por víctima. Así que por unos ciento treinta dólares, los timadores pueden generar dieciséis mil dólares, un retorno de la inversión del 12 000 por ciento[35]. Con treinta y seis mil millones de mensajes de *phishing* enviados cada año, la escala, el alcance y la rentabilidad de los ciberdelitos es palpable. Pese a que los ingresos obtenidos con estos ataques de *phishing* a gran escala son impresionantes, se quedan en mantillas en comparación con los del *spear phishing* (literalmente, «pesca con arpón»), una técnica que no envía mensajes fraudulentos en masa a millones, sino

que selecciona con esmero a personas u organizaciones concretas.

Los ataques de *spear phishing* se han convertido en la herramienta predilecta para quienes cometen espionaje industrial, y los costes en estos casos pueden ser colosales, tal como descubrió el gigante de los refrescos Coca-Cola. En el marco de su expansión por Asia, Coca-Cola se hallaba en una fase avanzada de las negociaciones para adquirir la empresa china Huiyuan Juice Group. Todo progresaba según lo previsto con la adquisición, hasta que, de manera inexplicable, se desmoronó como un castillo de naipes. Había gato encerrado y Coca-Cola exigía respuestas. De ahí que iniciara una investigación exhaustiva del asunto y empezara a examinar el acuerdo en detalle, incluidas las comunicaciones entre Coke y los representantes de Huiyuan Juice Group. Al final, Coca-Cola descubrió que el gobierno chino había estado supervisando de manera agresiva el pacto e inmiscuyéndose en secreto en los planes e intenciones de puja de Coca-Cola. ¿Cómo obtuvieron los chinos el acceso que necesitaban? Manipulando la pantalla de Paul Etchells, el vicepresidente del Pacific Group de Coca-Cola.

Etchells abrió un correo electrónico manipulado para simular que el remitente era un ejecutivo sénior del Departamento Legal de Coca-Cola. El asunto era tentador: «Ahorra energía, ahorra dinero: del presidente ejecutivo de Coke». Etchells sabía que su jefe en Coca-Cola apostaba por el ahorro energético en la empresa (como también sabían los chinos que se habían infiltrado en los sistemas de información corporativa de Coca-Cola). Los atacantes modularon la realidad haciendo que el mensaje pareciera proceder de un colega de confianza, perteneciente a la red corporativa interna, con un asunto atractivo y que, en el contexto, tenía sentido. Cuando el vicepresidente de Coke ingenuamente hizo clic en el enlace, se descargó sin saberlo *software* malicioso en su estación de trabajo, incluido un registrador de pulsaciones del teclado que capturaba todo lo que el ejecutivo tecleaba[36]. Como consecuencia, los chinos pudieron descargarse multitud de archivos informáticos relacionados con el acuerdo. Y si bien Coca-Cola ha rehusado comentar públicamente «asuntos de seguridad», es evidente que un único ataque de *spear phishing* contra un cargo importante de la empresa le costó la adquisición por dos mil cuatrocientos millones de dólares del Huiyuan Juice Group chino. Ahora bien, Coke no es la única que ha sucumbido al *spear phishing*, pues éste se ha convertido en el método de ataque predilecto de los ciberdelincuentes y espías digitales, responsables de un 91 por ciento de todos los ciberataques dirigidos contra un objetivo concreto[37].

En la actualidad, los delincuentes pueden modificar lo que aparece en tu pantalla en tiempo real, incluso tus extractos bancarios. ¿Qué sucedería si el saldo de tu cuenta estuviera a cero y no lo supieras? Hay tantos miles de programas de *software* malicioso que pueden robarte dinero del banco en la actualidad, que el proceso en su conjunto se ha convertido en una rutina automatizada. Los delincuentes infectan tu ordenador o teléfono móvil, capturan tus credenciales de inicio de sesión y luego las utilizan para vaciar tu cuenta bancaria. Por descontado, es posible que tú también te

conectes ese día y, al ver tu saldo, notifiques el asunto al departamento de fraudes de tu entidad bancaria y detengas la salida de fondos. Los bancos suelen reservarse uno o dos días de margen de actuación, sobre todo cuando se trata de operaciones internacionales, durante los cuales pueden cancelar, detener o revertir una transferencia o un traspaso, pero esa ventana de tiempo es increíblemente breve. Con este fin, los delincuentes despliegan todas sus armas para asegurarse de que lo que veas en pantalla no sea un reflejo de tu cuenta bancaria. *Software* troyano ultraespecializado, como SpyEye y URLZone, no sólo te roba dinero, sino que además te muestra extracto falsos de tu cuenta bancaria[38]. La magia de estos troyanos es que brindan a los ladrones más tiempo para utilizar tu información bancaria, de débito y crédito sin que te des cuenta de qué sucede. La primera pista que tienes de que existe algún problema es cuando intentas utilizar tu tarjeta para sacar dinero y el banco te informa de que no dispones de fondos suficientes.

El *crimeware* (*software* criminal o delictivo) involucrado es tan sofisticado que incluso sabe cuánto se ha robado de cada cuenta bancaria vulnerada. Así, si los ladrones robaron 2419 dólares de tu cuenta corriente, un algoritmo añadirá esa porción a lo que aparece en tu pantalla en tiempo real cuando compruebes el saldo de tu cuenta en Internet[39]. Las compras realizadas por los delincuentes con tu tarjeta de crédito o débito se eliminarán de manera automática de la lista de transacciones recientes y del extracto en línea antes de que aparezcan en tu pantalla. Incluso los archivos en PDF de los extractos de tu tarjeta de débito o crédito que envíes a imprimir se modificarán antes de salir por la impresora. Cuando estos ladrones te tienen en sus redes, eres suyo.

Estos tipos de ataque *man-in-the-middle* o con intermediario constituyen poderosos recordatorios de que los *hackers* delincuentes son perfectamente capaces de alterar la realidad que se te presenta a través del número creciente de pantallas que pueblan tu vida. Al igual que los artífices de Stuxnet, los delincuentes saben que las pantallas no son más que una representación de la realidad completamente maleable y fácilmente manipulable. Sin embargo, no toda la manipulación de los datos que vemos en pantalla la perpetran cárteles de ciberdelincuentes internacionales ni servicios de espionaje.

Es habitual que los pedófilos asuman identidades de niños, y los menores de dieciocho años son incapaces de discernir si están hablando con un adulto el 80 por ciento de las veces, lo cual hace que las pantallas de los niños sean especialmente vulnerables a ataques. Recuerda el caso de Amanda Todd, la niña de doce años a quien convencieron de que enseñara los pechos ante la videocámara, pensando que hablaba con un muchacho de su edad. Su atacante virtual la sobornó y atormentó en tal grado que la joven estudiante canadiense acabó quitándose la vida. Durante años, su caso permaneció abierto y los padres de Amanda no supieron quién había atormentado a su hija hasta abril de 2014, cuando una novedad en el caso condujo a la Policía Montada Real canadiense a los Países Bajos y hasta un sospechoso situado

a ocho mil kilómetros de distancia. La policía holandesa identificó a Aydin Coban, de treinta y cinco años, y lo acusó de «extorsión, señuelo en Internet, acoso delictivo y posesión de pornografía infantil con fines de distribución»[40]. Al parecer, el *modus operandi* de Coban consistía en crearse una identidad virtual falsa, granjearse la confianza de niñas y luego seducirlas para que realizaran actos sexuales delante de una *webcam*[41]. Se cree que el pedófilo holandés atacó a docenas de víctimas tanto en Canadá como en el resto del mundo[42].

Incluso para los adultos, las relaciones interpersonales y la manipulación de las pantallas puede ser una combinación explosiva. Tal fue el caso de Elizabeth Thrasher, a quien se acusó de agredir verbalmente a la hija de la nueva novia de su exmarido. Al parecer, la mujer, movida por los celos, copió dos fotografías de la cuenta de Myspace de la adolescente y las publicó en la sección de «encuentros esporádicos» del sitio web de Craigslist[43]. Luego especificó la dirección del domicilio de la muchacha, su número de teléfono, correo electrónico e información de su trabajo, aclarando que buscaba mantener relaciones sexuales. La presa de Thrasher supo de la publicación en Craigslist cuando empezó a recibir llamadas telefónicas, mensajes de texto y fotografías (incluidos desnudos), así como solicitudes de relaciones sexuales. En los tribunales, la muchacha testificó que se sintió como si «le hubieran tendido una trampa para que alguien la violara y la matara».

Apantallar los mercados bursátiles

Pero no sólo es posible manipular lo que aparece en las pantallas de personas y empresas, sino también de los mercados financieros. Si bien en el pasado los parqués se movían por rumores y suposiciones, la velocidad vertiginosa de Internet implica que el mundo a menudo reacciona antes de que se haya verificado la información. En agosto de 2000, un *hacker* llamado Mark S. Jakob, un estudiante universitario de veintitrés años de edad de El Segundo, California, creó una nota de prensa falsa y la envió a Internet Wire, un distribuidor de comunicados empresariales en Internet. Jakob eligió a Emulex Corporation, un fabricante de material de comunicaciones del Nasdaq, como su objetivo. El *hacker* se limitó a copiar el diseño y el estilo de comunicados de prensa previos de Emulex, imitó la dirección de correo electrónico de la empresa y envió su noticia a Internet Wire. Aquella nota de prensa ficticia aseguraba que la Securities and Exchange Commission (Comisión de Valores de Estados Unidos, conocida como SEC por sus siglas en inglés) había abierto una investigación contra Emulex, que sus ingresos trimestrales serían recalculados y que el director ejecutivo de la empresa, Paul Folino, había dimitido. Aquella noticia sensacionalista se volvió viral y fue recogida por otras agencias de prensa, incluidas

entre ellas TheStreet.com, CNBC, Bloomberg y Dow Jones Newswires[44].

La respuesta del mercado fue tan predecible como inmediata. «Apenas dieciséis minutos después de que otras agencias de prensa se hicieran eco de la nota de prensa falsa se vendieron 2,3 millones de acciones de Emulex cuyo precio cayó en picado 61 dólares, de 104 a 43, por lo que Emulex perdió 2200 millones de dólares en capitalización de mercado[45]» Justamente la reacción que Jakob había esperado obtener cuando vendió al descubierto el valor bursátil, lo cual reportó al joven manipulador de los parqués una plusvalía latente de 250 000 dólares[46]. El director ejecutivo de Emulex apareció de inmediato en Bloomberg y en otros medios de prensa económica desmintiendo la noticia, pero para entonces el daño ya estaba hecho. Al cabo de seis días, el FBI, en colaboración con la SEC, había identificado a Jakob, que fue arrestado y declarado culpable de delito informático y fraude en las cotizaciones[47].. Una vez aclarado el asunto, los inversores legítimos en el mercado perdieron más de 110 millones de dólares porque un chaval en un centro de estudios superiores manipuló la confianza que tenían en sus pantallas.

La manipulación de las pantallas en el sector de los servicios financieros es moneda corriente y los llamados programas de *pump-and-dump*[*] son el bistec con patatas del fraude en las cotizaciones en Internet. Esta práctica consiste en que los negociantes inflan de manera artificial el precio de un valor bursátil publicando en línea declaraciones positivas falsas o engañosas y luego venden las acciones antes de que sus mentiras se descubran y su precio se desplome[48]. Esta práctica ha florecido en el ciberespacio y el FBI ha arrestado a docenas de delincuentes por participar en estas estafas. Pese a que el planteamiento del *pump-and-dump* por regla general adolece de sofisticación, tanto personas individuales como la delincuencia organizada se han embolsado centenares de millones de dólares manipulando la información que vemos en Internet[49].

En ocasiones, las pantallas financieras pueden manipularte sin que te des cuenta de ello, observándote a la par que tú las observas. Eso fue lo que los agentes de bolsa expertos de Goldman Sachs y JPMorgan descubrieron acerca de los terminales de compraventa de acciones Bloomberg que usaban desde hacía años[50]. Los terminales de Bloomberg son la savia de Wall Street y las empresas pagan 20 000 dólares por año y terminal por la minería de las toneladas de datos que proporcionan con vistas a efectuar sus operaciones bursátiles a diario. No obstante, lo que estos agentes de bolsa desconocían es que a los periodistas del Departamento de Prensa de Bloomberg se les había concedido acceso como administradores a esos terminales, lo cual les permitía monitorizar las actividades de los clientes cuando los agentes de bolsa los utilizaban. Dicho de otro modo, los periodistas de Bloomberg supervisaban el uso de los terminales para estar siempre al filo de la noticia. Los agentes de bolsa que creían estar visualizando información de manera privada en un terminal mudo descubrieron que ese terminal de hecho era muy locuaz y se dedicaba a observarlos.

Más de 300 000 de las personas más influyentes en el mundo financiero, incluidos banqueros, administradores de fondos de cobertura y funcionarios del Departamento del Tesoro confían en estas cajas de Bloomberg para realizar sus exhaustivas pesquisas privadas, en las que cada búsqueda está vinculada a una persona concreta. El escándalo salió a la luz cuando un periodista de Bloomberg telefoneó a Goldman Sachs para preguntar si un socio seguía trabajando en la empresa, alegando que hacía días que no se conectaba a su terminal. Aquel comentario trivial hizo que sonaran las alarmas en Goldman Sachs, que hizo pública la noticia.

Posteriormente se reveló que dos mil cuatrocientos periodistas de Bloomberg estaban autorizados a ver el historial de inicio de sesión de los usuarios en los terminales de la empresa, así como las distintas funciones de búsqueda que empleaban, como patrimonio neto y productos básicos[51]. Los directivos de Goldman lamentaron que los periodistas de Bloomberg hubieran espiado a hurtadillas a sus clientes mediante sus terminales y hubieran empleado aquella información privada para espiar la actividad de los socios de Goldman, información que usaban para generar noticias para Bloomberg[52]. Un antiguo periodista de Bloomberg afirmó que «en la sala de prensa siempre se debatía cómo utilizar los terminales para publicar una primicia»[53].

Las pantallas financieras también pueden piratearse y manipularse mediante negociaciones de alta frecuencia. En su imprescindible libro de 2014, *Flash Boys: la revolución de Wall Street contra quienes manipulan el mercado*, Michael Lewis explica cómo los expertos de Wall Street han engañado a todo el sistema de operaciones financieras pirateando el tiempo. Mediante la inversión de centenares de millones de dólares en una infraestructura técnica muy superior, los agentes de bolsa de alta frecuencia conseguían rascar apenas milisegundos en sus tiempos de compraventa, lo cual les proporcionaba una ventaja operativa frente a sus colegas. *Flash Boys* narra la historia de Brad Katsuyama, un agente de bolsa de la oficina neoyorquina del Royal Bank of Canada, y su complejísima investigación de varios años de duración en el ámbito de las negociaciones de alta frecuencia[54]. Lo que descubrió fue desconcertante: el mercado bursátil tal como se mostraba en las pantallas de su escritorio era una ilusión.

Al parecer, cada vez que Katsuyama intentaba efectuar una negociación, el precio de la acción cambiaba antes de que su orden se hubiera completado. ¿Cómo era posible? Unos agentes bursátiles que trabajaban a gran velocidad habían descubierto un modo de aprovechar las velocidades variables a las que la información de las operaciones bursátiles se desplazaba por los cables de fibra óptica hasta las bolsas de valores. Aunque las señales viajaban a dos tercios de la velocidad de la luz, al recorrer largas distancias esos lapsos minúsculos iban sumándose y podían aprovecharse. Pagando inmensas sumas de dinero por los cables más veloces, los ordenadores más potentes y el privilegio de colocar sus servidores de datos en el seno

de los propios mercados bursátiles, aquellos agentes de bolsa de alta frecuencia eran capaces de detectar la intención de Katsuyama de adquirir una acción a un precio de ejercicio determinado y adquirirla antes que él al precio que aparecía en su pantalla. Katsuyama no era el único afectado, sino que el problema nos afectaba a todos, pero él fue el primero en documentarlo. Los negociadores de alta frecuencia ocupaban los puestos de avanzadilla en los mercados y, por ende, nos fastidiaban a todos, incluido a ti y a tus fondos de inversión inmobiliaria, a tu plan de ahorro e incluso a los planes de pensiones municipales.

Los negociadores de alta frecuencia habían pirateado el tiempo y las pantallas en lo que supuso un ataque con intermediario sin paliativos. Se colocaron entre los datos de los mercados bursátiles supuestamente suministrados a tiempo real proyectados en las pantallas de Katsuyama y una realidad mucho más veloz, que controlaban y poseían. Sus ordenadores eran tan rápidos que podían detectar las órdenes de otras personas, colarse por delante de ellas, comprar las acciones en cuestión y vendérselas a la persona que había intentado adquirirlas originalmente, pero a un precio superior. Una diferencia de unos cuantos peniques por aquí y por allá en millones de valores bursátiles al día permitía a los negociadores de alta frecuencia amasar miles de millones de dólares en beneficios acumulativos gracias a una ventaja comercial de cinco milisegundos. Para contextualizar tal nivel de velocidad, baste decir que el parpadeo de un ojo humano tarda entre trescientos y cuatrocientos milisegundos. Es similar a la escena de la película *Matrix* en la que los malos empiezan a disparar a Neo (Keanu Reeves) y él puede ver las balas acercándose y moverse a la velocidad de la luz para esquivarlas, salvo por el hecho de que en este caso se trata de vulnerar el sistema financiero y ninguno de nosotros, simples mortales, tenemos los poderes de Neo.

En la estela de la publicación de *Flash Boys*, la SEC, el FBI y el fiscal general del estado de Nueva York lanzaron una serie de investigaciones. Sin embargo, su interés repentino abre un interrogante importante: ¿cómo es posible que todo este sistema pudiera desarrollarse a plena vista de la SEC justo después de la crisis financiera mundial de 2008? Como tan oportunamente señaló Michael Lewis, el «mercado está amañado», pero antes de que esto sucediera, las empresas implicadas en las órdenes relámpago tenían que sabotear tu pantalla para poder crear la ficción de un mercado bursátil transparente y de confianza. Desconcierta saber que vivimos en un mundo en el que las pantallas de los hospitales, las cárceles, los departamentos policiales, los bancos, los agentes de bolsa y los sitios web de noticias son tan fáciles de vulnerar. Pese a ello, tal como comprobaremos, las pantallas proliferan, las amenazas aumentan y estos ataques pueden costarnos mucho más que dinero.

Capítulo 9

Cuantas más pantallas, más problemas

> En un mundo que cada día se desconecta más de la verdad, cada vez más personas aceptan lo virtual frente a lo real, y todo lo virtual es también maleable.
>
> DEAN KOONTZ, *The good guy*

Robin Sage era una joven atractiva de veinticinco años que trabajaba como analista de ciberamenazas en el Network Warfare Command de la Marina estadounidense. Era licenciada por el MIT y hacía prácticas en la NSA. Como tantas personas de su edad, Robin era una usuaria consumada de las redes sociales, con perfiles en Facebook, LinkedIn y Twitter. Poco después de iniciar su carrera en la Marina, empezó a enviar solicitudes de amistad a otros ciberexpertos que trabajaban para el gobierno estadounidense. En poco menos de un mes, su red se había ampliado en más de trescientos contactos entre el mundo de la ciberseguridad, incluyendo personal militar, contratistas de Defensa y personal de varios organismos de inteligencia y espionaje. Entre sus nuevos colegas online figuraba el presidente de la Junta de Jefes de Estado Mayor de Estados Unidos, el gerente de sistemas de la NSA, funcionarios sénior de inteligencia del Cuerpo de los Marines, el jefe de personal de un congresista estadounidense y ejecutivos de Lockheed Martin, Northrop Grumman y Booz Allen Hamilton.

Pese a que muchos destinatarios de sus solicitudes de amistad al principio no recordaban a la joven, Robin les aseguró que se habían conocido el año anterior en el DEF CON, un importante simposio sobre pirateo informático frecuentado por *hackerati* (piratas informáticos de alto nivel) y espías gubernamentales por igual. Aquellos que albergaban dudas echaron un vistazo a la red de Robin y comprobaron que tenían multitud de amigos en común, lo cual disipó cualquier temor a aceptar su solicitud de amistad. Robin incluso contactó por Facebook y LinkedIn con quienes trabajaban con ella en el mismo edificio del Naval Network Warfare Command. A medida que su red y su presencia en las redes sociales se amplió, Lockheed Martin y otras empresas mostraron interés en contratar a la joven para trabajar para ellos y le empezaron a llover ofertas de empleo. Sólo había un pequeño problema: Robin Sage no existía[1].

Sage era una invención de Thomas Ryan, un asesor en materia de seguridad que quería comprobar las amenazas que las redes sociales planteaban para los profesionales que trabajaban en la comunidad de la seguridad nacional[2]. Su objetivo era muy sencillo: comprobar cuánta información privilegiada podía recabar de

manera encubierta a través de las redes sociales mediante una identidad ficticia. En menos de un mes, sus nuevos contactos comenzaron a compartir abiertamente amplios datos con su atractiva *alter ego*, Robin Sage. Desplegando una rutina virtual a lo Mata Hari, Ryan embaucó a un soldado del Cuerpo de Operaciones Especiales estadounidense con quien había contraído amistad para que enviara fotografías a Sage…, fotografías que incluían datos de geolocalización de su base secreta en Afganistán. El soldado reveló, además, detalles acerca de sus movimientos y otros movimientos de tropas en Irak a su nueva «amiga».

La presencia en la pantalla de Robin Sage era tan convincente que incluso recibió documentos confidenciales para revisar y ofertas para hacer ponencias en varias conferencias de alto nivel sobre ciberguerra y ciberseguridad. ¿Le resultó muy arduo a Ryan organizar este ardid contra un grupo de élite de profesionales avezados de la esfera militar y de la inteligencia de la comunidad estadounidense dedicada a velar por la seguridad nacional? Fue coser y cantar. Ryan se limitó a escoger una fotografía en Internet y la utilizó para crear los perfiles de Sage en las redes sociales. En realidad, la fotografía pertenecía a una actriz porno poco conocida con una reputación limitada. Incluso su nombre, Robin Sage, era en realidad el nombre de un extenso ejercicio militar que el Ejército lleva a cabo anualmente en Carolina del Norte. ¿Y la dirección postal de Robin? La del infame contratista de seguridad militar del Blackwater. El experimento de Robin Sage demuestra la facilidad con la que puede socavarse la confianza que las personas depositan en sus pantallas. Si profesionales militares y espías entrenados mordieron el anzuelo, ¿qué posibilidades tiene el público general de protegerse ante esta suerte de amenazas? Ahora bien, cuando todo está conectado, los ordenadores distan mucho de ser las únicas pantallas de las que hay que preocuparse.

Filtrado de llamadas

Habida cuenta de la proliferación desmedida de dispositivos móviles, no sorprende que los delincuentes estén desviando su atención de las grandes pantallas a las más pequeñas, sobre todo porque el *software* de los teléfonos suele ser menos seguro que el de los ordenadores de sobremesa. Pese a que todos estamos acostumbrados a ver la identidad de quién nos llama en las pantallas del teléfono móvil, de los teléfonos del despacho y también del de nuestro domicilio, como todas las pantallas, éstas son fácilmente pirateables. Existen multitud de programas informáticos y sitios web destinados a alterar la identificación de la persona que llama.

Sitios web y aplicaciones móviles como SpoofCard.com y SpoofTel.com permiten configurar el teléfono fácilmente para que muestre un número distinto al efectuar una llamada. Para ello, basta con introducir el número y el nombre que se

desea que el destinatario de la llamada vea en la pantalla. ¿Te interesa fingir que eres el presidente de Estados Unidos? Ningún problema. Basta con escribir: «202-456-1414» y «La Casa Blanca» en la aplicación ¡y listos! Las empresas de fraude telefónico ponen a tu disposición una amplia variedad de paquetes destinados a confundir otro sentidos, además de la vista. Así, ofrecen la capacidad de mutar tu voz masculina en femenina e incluso de insertar ruido de fondo en una conversación para convencer a la otra parte de que telefoneas desde una oficina ajetreada, una discoteca, un atasco de tráfico o un aeropuerto. Estas empresas promocionan sus productos como un medio de «proteger tu identidad» o «gastar bromas a tus amigos». Por descontado, los mensajes de texto también pueden alterarse aplicando estas mismas técnicas. Si bien no cabe duda de que los adolescentes se divierten fingiendo ser cualquier persona, desde Lady Gaga hasta el director del FBI, evidentemente también existen usos más perversos que los delincuentes están más que dispuestos a aprovechar.

En el caso del la debacle épica de pirateo telefónico de News Corp, una pantalla con identificación de llamadas pirateada permitió a los periodistas acceder al sistema de buzón de voz de Milly Dowler, entre otros, un ataque que bien podría sucederte a ti. La estafa funcionó porque, por omisión, muchas teleoperadoras móviles no exigen contraseña para acceder al buzón de voz. El sistema simplemente confía en la identidad de quien efectúa la llamada para comunicarle sus mensajes. Puesto que todas las empresas móviles de todo el mundo cuentan con un número 800 central al cual puedes telefonear cuando llamas desde una línea fija, los malos se limitan a hacerse pasar por tu número telefónico a la hora de telefonear al sistema de buzón de voz de la operadora y, ¡bingo!, obtienen acceso pleno a tus mensajes. Con esta técnica no sólo se ha espiado a figuras públicas del Reino Unido, sino que también personas famosas en busca de cotilleos la han empleado para colarse en los buzones de voz de sus rivales, como el célebre caso en el que Paris Hilton utilizó SpoofCard para escuchar los mensajes de Lindsay Lohan[3].

En el mundo real de los ciudadanos corrientes, el hecho de que suplanten tu identidad telefónica permite a los delincuentes escuchar tus mensajes de la oficina y obtener información valiosa relativa a operaciones empresariales pendientes, fusiones y adquisiciones, e incluso datos médicos personales. Desde la perspectiva de la ingeniería social, los fraudes telefónicos constituyen una potente herramienta para la mente delictiva. Una llamada con identidad falsa al departamento de tecnologías de la información de una empresa solicitando el cambio de una contraseña o la última clave Wi-Fi probablemente obtendrá mejores resultados si la llamada parece proceder de la infraestructura telefónica interna de la propia empresa, una estratagema que siempre da resultado.

En la esfera personal, el hecho de alterar la identidad de la llamada entrante en tu teléfono también es una herramienta eficaz para los timos bancarios. Instituciones bancarias como Bank of America y Chase ofrecen banca por telefonía, y son legión

los delincuentes que fingen llamar desde la cuenta a la cual desean acceder. Una vez el sistema telefónico del banco detecta una llamada entrante desde tu número de teléfono, lo único que precisan los malos son unos cuantos datos personales (como los últimos cuatro dígitos de tu número de la Seguridad Social o el apellido de soltera de tu madre), información facilísima de conseguir tanto en la clandestinidad digital como en tu perfil de Facebook, y ya están dentro[4]. Peor aún, los delincuentes pueden fingir llamarte desde el número telefónico de tu banco y solicitarte que les facilites determinados datos, como tus preguntas de seguridad, y luego invertir los roles y llamar a tu banco utilizando tu número de teléfono ficticio y los datos de seguridad que ingenuamente les has proporcionado para acceder a tu cuenta[5].

La delincuencia organizada ha conseguido incluso fingir llamar desde el gobierno federal de Estados Unidos y, con ello, han amasado millones de dólares. En lo que el Servicio de Impuestos Internos (IRS por sus siglas en inglés) describió como su estafa fiscal de mayor envergadura hasta la fecha, los estafadores fingieron llamar a los ciudadanos desde el número telefónico de la Agencia Tributaria[6]. Cuando uno ve una llamada entrante del IRS, piensa: «¡Maldita sea! ¿Qué pasa?». Al otro lado del aparato, un funcionario le acusa de ser un evasor de impuestos y lo conmina a abonar inmediatamente los pagos debidos para evitar incurrir en multas adicionales. A las víctimas de este timo se les dice que «dada la gravedad del delito y sus antecedentes delictivos, únicamente aceptaremos pagos mediante transferencia bancaria o tarjetas de débito de prepago». Para dotar de más credibilidad a la estafa, los supuestos agentes del IRS confirman los cuatro últimos dígitos del número de la Seguridad Social del contribuyente (filtrados en uno de los múltiples ataques masivos descritos con anterioridad). Y quienes dudan de la veracidad de la llamada son objeto de un torrente de amenazas, que van desde arresto hasta revocación de sus licencias empresariales o del permiso de conducir e incluso deportación si su nombre o acento delata que son extranjeros.

Los estafadores apuntalan la veracidad de sus afirmaciones pirateando otras pantallas y añadiendo nuevos jugadores en forma de bits a su ardid. A continuación, las víctimas suelen recibir mensajes de correo electrónico de aspecto oficial con un «membrete del Servicio de Impuestos Interno» que confirman la llamada y exigen que se efectúe el pago. Además, reciben llamadas adicionales de la policía local con la identidad alterada (por ejemplo: «Departamento de Policía de Amherst, Massachusetts») o de supuestos funcionarios estatales de la Dirección General de Tráfico (por ejemplo, la DGT del estado de Georgia). Estos «funcionarios» adicionales confirman el timo con guiones como: «Al habla el detective Smith del Departamento de Policía de Amherst. Acabamos de recibir una notificación del IRS indicando que ha cometido usted fraude fiscal y un delito penal. No quiero tener que acudir a arrestarle delante de su familia. Si efectúa usted el pago esta semana, el IRS me indica que no será necesario arrestarlo». De acuerdo con el inspector general del Departamento del Tesoro, más de veinte mil personas han sido víctimas de esta

estafa.

Ahora bien, la confianza en la pantalla puede costarte mucho más que dinero, incluso la vida. En un fenómeno conocido como *swatting* o broma pesada, los *hackers*, aburridos, se dedican a telefonear al número de emergencias de la policía con identidades telefónicas falseadas para informar de delitos inexistentes, lo cual pone en funcionamiento a unidades especiales de policía armada hasta los dientes. Aunque el pirata informático puede encontrarse en Maine, al utilizar tu número de teléfono de Miami, ahí es donde se dirige la policía. Este juego mortal comienza cuando los delincuentes falsean tu número telefónico y llaman desde él a emergencias. Una mujer grita por el teléfono: «Mi marido acaba de disparar a mi madre y mi bebé y ahora me tiene retenida como rehén… Por favor, vengan rápido… Tiene una metralleta y un AK-47…¡Dense prisa! ¡Se ha vuelto loco!». De fondo suena la grabación de un tiroteo para mayor credibilidad. Y la trampa mortal ya está servida.

Entre tanto, tú estás sentado en tu casa tranquilamente, comiendo helado en el sofá con tu esposa y tus hijos mientras miráis el último episodio de *Big Bang*. La policía cree que la mujer en el interior de la casa podría morir en cuestión de segundos y envía a todos los agentes disponibles y una unidad de las fuerzas especiales a rescatarla. Cuando ambos bandos se encuentran, hay una profunda disonancia cognitiva y el encuentro se convierte en un peligroso polvorín. La policía tiene rodeada la casa y te apremia a salir con las manos arriba. Tus hijos gritan y tu mujer se muestra confusa. Además, al no acatar las órdenes de la policía, ésta presagia que está sucediendo algo terrible en el interior de tu hogar. No te apetece salir de tu casa y enfrentarte a un grupo de locos (aunque sean policías) que te apuntan con sus rifles. Para la policía, tu negación a colaborar sólo incrementa la tensión. El paso siguiente es lanzar algunas granadas de aturdimiento por la ventana hacia el interior de tu domicilio y esperar a ver qué ocurre. También podría pasar que estuvieras dormido cuando el pirata informático adolescente decide gastarte la broma pesada desde varios estados de distancia. La policía se presenta en tu casa y te despiertan los ruidos al otro lado de la ventana. Crees que se trata de ladrones y agarras tu arma para salir a investigar. En cuanto sales a la calle con un arma en la mano, seis miembros del equipo de las fuerzas especiales local te apuntan con láseres rojos a la frente. Es imposible que la situación acabe bien.

El FBI registró al menos cuatrocientos incidentes de *swatting* sólo en 2013, con víctimas en todo Estados Unidos, desde Ohio hasta California[7]. En la mayoría de los casos, son *hackers* que buscan «echarse unas risas» quienes gastan estas bromas pesadas, porque pueden hacerlo. En los días previos a Internet, la broma más pesada que podía gastar un adolescente consistía en encargar *pizzas* por teléfono y enviarlas a casa del compañero de la escuela que no le caía bien. Ahora los chavales envían unidades de las fuerzas policiales especiales con armas a ejecutar sus inocentadas. Por ejemplo, en 2009, un grupo de adolescentes de Massachusetts fueron condenados

por llevar a cabo más de trescientos ataques de *swatting*. En algunos casos, los adolescentes coincidieron con sus víctimas en redes sociales o en sitios web de citas y se vengaron de ellas si, por ejemplo, se negaron a entablar conversaciones sexualmente explícitas con ellos[8]. De hecho, el *swatting* es el complemento ideal de las ofertas de sexo ficticias que las exparejas celosas publican en Craigslist para clamar venganza contra sus examantes, y las pone aún en un riesgo mayor[9].

Cada vez son más los personajes famosos y las figuras públicas de alto perfil acosados por esta práctica. En 2013, un niño de doce años fue juzgado en Los Ángeles por perpetrar ataques de *swatting* contra el domicilio en Hollywood de Ashton Kutcher y la finca de Justin Bieber en Calabasas, California. También telefoneó a la policía para informar de un atraco en un banco local[10]. Otras víctimas famosas de este tipo de ataques son Russell Brand, Tom Cruise, Rihanna, Charlie Sheen y Miley Cyrus. Ha sido un milagro que no haya muerto ningún civil inocente a resultas de estos incidentes, si bien algunos agentes de policía sí que han resultado heridos mientras arriesgaban sus vidas para reaccionar a toda velocidad a espeluznantes llamadas falseadas a los servicios de emergencia[11].

Otro modo que los delincuentes tienen de subvertir la pantalla de tu teléfono es atacando su banda base, es decir, las entrañas responsables de que funcione. La banda base gestiona toda la comunicación entre lo que ves en la pantalla y una serie de antenas de radio que lo controlan todo, desde los mensajes de texto que recibes hasta tus llamadas de voz y la señal del Wi-Fi, además de protocolos de telecomunicaciones superespecializados como GSM, UMTS, HSDPA y LTE[12]. Puesto que la banda base es privada y restringida, la mayoría de los fabricantes de teléfonos implantan estos sistemas operativos subyacentes sin preocuparse por la seguridad. Confían en la seguridad que garantiza la oscuridad: este *software* es tan, tan interno que nadie puede detectarlo y, por consiguiente, no es preciso preocuparse de que sea seguro, les dice la lógica. Por supuesto, se equivocan.

Piratas informáticos, gobiernos e investigadores en materia de seguridad han comenzado a revertir con éxito la ingeniería de los chips y el código de las bandas base, gracias a lo cual han dejado al descubierto un amplio abanico de vulnerabilidades de la seguridad que pueden utilizarse para acceder y modificar de manera remota datos de un teléfono[13]. A principios de 2014 se detectó un fallo en la seguridad y un puerta trasera de este tipo en el *software* de la banda base de los teléfonos Samsung Galaxy, los cuales permitían a los piratas informáticos acceder a los datos de los usuarios almacenados en los dispositivos[14]. Puesto que los *smartphones* actuales no son más que ordenadores en miniatura, sus pantallas, como las de sus camaradas de mayor tamaño, pueden manipularse para mostrar una realidad alterada con fines engañosos. Según consta, el FBI ha utilizado esta técnica para convertir teléfonos en dispositivos de vigilancia oculta modificando la interfaz habitual del dispositivo y haciendo que realizara una llamada clandestina al FBI para

permitir la monitorización remota[15]. En otras palabras, aunque en el dispositivo sólo se viera la pantalla de inicio con las aplicaciones, en realidad estaba telefoneando a los federales que estaban a la escucha.

Los delincuentes también pueden manipular estas pantallas del mismo modo, a menudo empleando técnicas que ni se nos pasan por la cabeza. Por ejemplo, cuando marcas un número en el dispositivo móvil, lo haces pulsando una serie de números en la pantalla para conectar con el destinatario. Pero ¿cómo sabes que el número que has marcado es el número con el que has conectado? Es bastante sencillo saberlo si llamas a tu madre y ella descuelga. Pero ¿qué sucede si llamas a tu entidad bancaria, a Citibank, Bank of America o Wells Fargo? Hoy en día ya no acudes a la sucursal bancaria del barrio, como hacíamos veinte años atrás. En su lugar, te conectan a alguien con quien nunca antes has hablado que se encuentra en un centro de atención al cliente, generalmente localizado en un país extranjero y gestionado por personas con acentos foráneos.

Utilizando *malware* para teléfonos móviles, los piratas informáticos pueden instalar un *rootkit* en tu teléfono que les permite controlar todas las funciones del dispositivo, incluida la pantalla táctil y el teclado numérico. Los *rootkits* son programas maliciosos que ocultan las funciones y los procesos informáticos normales de la vista del usuario y brindan a los piratas informáticos acceso como administrador o «usuario root» a cualquier dispositivo. Las mafias conocen los números 800 de las entidades bancarias de todo el mundo. Si infectan tu teléfono con *malware,* cuando llamas al número de atención al cliente de tu banco, el *rootkit* detecta que estás telefoneando a una de las instituciones definidas como objetivo, intercepta y reconduce la llamada. Se trata de otro ataque con intermediario clásico que permite a los delincuentes moldear la realidad que ves en la pantalla y obtener el resultado que pretenden.

En consecuencia, cuando marcas el 1-800-4MI-BANCO, tu llamada se desvía de manera invisible a un centro de atención telefónica dirigido y operado por una mafia internacional. Dado el amplio uso que las instituciones bancarias hacen de centros de atención al cliente deslocalizados, ¿a quién le extrañaría que le responda alguien con acento extranjero al otro lado del aparato cuando habla con «su banco»? La estafa es bastante fácil de llevar a cabo. Una vez te conectan, te preguntan tu número de cuenta, tu nombre completo, tu contraseña y otra información de seguridad «para verificar que se trata de ti». A continuación te dicen: «Lo lamento, señor, el sistema informático ha dejado de funcionar. El departamento técnico nos informa que volverá a estar operativo por la mañana. ¿Le importa volvernos a telefonear entonces?». Nada en esta conversación sonaría sospechoso a nadie que hubiera telefoneado a los empleados de un centro telefónico en el pasado. La única diferencia estriba en que, cuando la llamada concluya, el delincuente tendrá acceso pleno a tus datos personales y bancarios y los utilizará a toda prisa para sustraer todos los fondos de la cuenta. Todo esto es posible porque las pantallas de nuestros teléfonos móviles no nos

muestran la realidad, sino una aproximación de ésta. Debido a ello, no sólo es posible piratear la identidad de la persona que nos llama y el sistema operativo de un dispositivo móvil, sino también sus otras funciones, incluidos los módulos de GPS. En efecto, también puede modificarse tu localización.

Perdidos en el espacio: GPS manipulados

En la película de James Bond de 1997 *El mañana nunca muere*, el agente secreto investiga la manipulación del sistema de navegación por GPS de una fragata británica. En el argumento, un genio diabólico utiliza una «caja de codificación» para alterar la navegación del *HMS Devonshire* y desviar el buque de su ruta. En consecuencia, el *Devonshire* penetra en aguas territoriales chinas y, supuestamente, la Marina china lo hunde. Sin embargo, para los británicos, la fragata se hallaba claramente en aguas internacionales y, por ende, los chinos han cometido un acto de guerra. Las acciones del villano tienen el efecto que pretendía: Gran Bretaña y China se internan por la senda del conflicto bélico. Una vez más, Hollywood fue clarividente en su visión del mal del futuro.

El sistema de posicionamiento global o GPS (siglas en inglés de Global Positioning System) es una «constelación de 24 satélites de navegación» que orbitan en el espacio cerca de la Tierra y proporcionan información sobre la localización y hora en cualquier punto del planeta. Se trata de una «utilidad invisible» en la que confiamos para desplazarnos por la ciudad, entregar paquetes, encontrar la cafetería Starbucks más cercana, coordinar el control del tráfico aéreo, gestionar la seguridad pública e incluso guiar misiles. Los mapas en papel han quedado obsoletos. En su lugar, hemos acabado por confiar en las pantallas de navegación que vemos ante nuestros ojos cada día y asumimos sin más que los ordenadores lo saben todo. De hecho, existen casos en todo el mundo de conductores que siguen a ciegas sus GPS en lugar de guiarse por sus dos ojos y acaban conduciendo en sentido contrario en una calle de una sola dirección o incluso saltan de puentes. En España, cuando el GPS indicó de repente a un hombre que girara a la derecha, éste lo obedeció sin más, se salió de la carretera y cayó en La Serena, el mayor embalse de la España occidental. Aunque el pasajero sobrevivió, el conductor se ahogó… todo por seguir las indicaciones de la pantalla[16].

Un informe del Departamento de Seguridad Nacional de Estados Unidos advertía de que las infraestructuras esenciales del país «eran cada vez más vulnerables debido a la creciente dependencia de los GPS en materia de posicionamiento y navegación»[17]. La nota de prensa de un informe similar realizado por la Royal Academy of Engineering del Reino Unido era aún más cruda en su aseveración: «La sociedad corre el riesgo de confiar demasiado en los sistemas de navegación por radio

satélite como los GPS […] Un fallo o una interferencia en la señal podría afectar a los sistemas de seguridad y partes vitales de la economía»[18]. Resulta ser que, de la misma manera que la ciberinfraestructura está poco protegida y, por ende, queda expuesta y es completamente vulnerable, lo mismo ocurre con nuestra infraestructura de espectros radioeléctricos y satélites.

El GPS es un logro tecnológico sensacional, pero las señales de GPS por satélite que recibimos en realidad, pese a ser perfectamente funcionales, son muy débiles, el equivalente a ver un faro de un coche desde veinte kilómetros de distancia. Esas señales no pueden reforzarse debido al suministro energético limitado de todos los satélites y, lo que es aún peor, pueden quedar solapadas por el ruido de las emisiones en la misma frecuencia y, por consiguiente, impedir que otros dispositivos con base terrestre reciban la información sobre navegación.

En el pasado, sólo las fuerzas militares avezadas en el arte de la «guerra electrónica» tenían acceso a la tecnología y los conocimientos para interceptar las señales de GPS[19]. Las implicaciones estratégicas de hacer tal cosa son evidentes. Si se logran bloquear los sistemas de navegación del enemigo, se puede interferir en el movimiento de sus tropas, buques, tanques y Marina. Y también se puede dañar gravemente la infraestructura nacional esencial civil del adversario. En Estados Unidos, tuvimos una pequeña ocasión de comprobarlo en enero de 2007 en San Diego, California, cuando toda la ciudad sufrió una «avería electrónica». En torno a mediodía, los controladores del tráfico aéreo descubrieron súbitamente que sus sistemas no funcionaban bien. En los hospitales locales, los buscas de los médicos dejaron de funcionar y, en el puerto de San Diego, la navegación de barcos se tambaleó. Durante dos horas enteras, los teléfonos móviles de toda la ciudad dejaron de funcionar y los cajeros automáticos dejaron de dar dinero. Lo más cerca de una película de Bruce Willis que se puede estar en la «mejor ciudad» de Estados Unidos. ¿Qué provocó aquel apagón generalizado? Durante tres días, aquel acontecimiento fue un misterio total, hasta que la Marina finalmente dio a conocer que había estado realizando un ejercicio de pruebas para probar una nueva tecnología de interferencia por radio. En ocasiones, las interferencias militares en las señales de GPS no son ningún accidente. Corea del Norte suele atacar a su vecino del sur y bloquear sus señales de GPS. Pyongyang utiliza tres aparatos de interferencias del tamaño de un tráiler que cambia de ubicación con el fin de bloquear la navegación por satélite en gran parte de Corea del Sur. El ataque a los GPS más dilatado perpetrado por Corea del Norte tuvo lugar a principios de 2012, se prolongó dieciséis días y obligó a modificar las rutas de 1106 aviones y 254 barcos[20]. Debido a la ley de Moore, la tecnología que emite las señales GPS es cada vez más pequeña, barata y potente. Por tanto, ya no sólo las fuerzas armadas tienen acceso a los interceptores de la navegación, sino que cualquier ciudadano corriente y moliente puede conseguir uno, con resultados notables para tu pantalla.

Pese a ser ilegales en Estados Unidos, los interceptores de GPS pueden

conseguirse fácilmente en Internet, en sitios web como www.jammer-store.com. Por sólo 50 dólares, cualquiera puede adquirir un modelo de salpicadero que se conecta al mechero del coche y crea una burbuja electromagnética que te envuelve mientras conduces[21]. Su uso es más popular de lo que imaginas. Cada vez son más las empresas que dotan de GPS a todos los vehículos de sus flotas comerciales. Ello permite a las empresas de transporte a larga distancia, empresas de mensajería, departamentos de policía, flotas de taxis, transportistas de coches blindados y proveedores de televisión por cable llevar un seguimiento de sus empleados, gestionar sus operaciones, fomentar el uso eficiente de combustible y cuantificar la productividad de su personal. A los trabajadores que conducen estos vehículos, esta supervisión mediante GPS les hace tener la sensación de que el Gran Hermano los observa. En respuesta a ello, estos empleados empezaron a sabotear los dispositivos cortándoles el cableado o arrancándoselo directamente. Por supuesto, se metieron en problemas con sus jefes. Ahora, un interceptor de cincuenta dólares consigue el mismo efecto y no deja huellas.

El problema de estos interceptores portátiles es que extienden esa burbuja protectora en un radio de 150 metros desde los vehículos en los que los usan. Eso implica que, dependiendo de la potencia del dispositivo, por cada camionero que no quiera que su jefe sepa que está echando una cabezadita, la señal de GPS de entre cincuenta y cien vehículos adicionales también quedará bloqueada. Ahora bien, la navegación de tu teléfono o coche en realidad es la red menos importante que el interceptor bloquea. Tal como comprobamos en el incidente de San Diego, pese a que no resultara evidente de manera inmediata, las torres de telefonía móvil, el tendido eléctrico, el control del tráfico aéreo y los cajeros automáticos también dependen de sistemas con GPS incorporado para funcionar correctamente. Cuando los camioneros locales se desconectan, desconectan también a muchas otras personas y servicios, y cada año se comunican cientos de incidentes de daños colaterales. Por ejemplo, en Londres, durante diez minutos al día, los agentes de Bolsa detectaban que sus operaciones no se realizaban porque había un problema con el mecanismo de datación del sistema[22]. El personal del mercado bursátil, desconcertado, se preguntaba si estaría siendo objeto de algún ciberataque externo. Pues no, era un camionero londinense que aparcaba su camión junto al parqué mientras efectuaba sus repartos una vez al día durante diez minutos.

Esta interrupción en Londres no es más que uno de los múltiples incidentes de este tipo que tienen lugar en todo el mundo. En Nueva Jersey, el gobierno había instalado un nuevo sistema de aterrizaje mediante GPS en el Aeropuerto Internacional Newark Liberty para permitir a los aviones aterrizar en condiciones de baja visibilidad. Por razones que se desconocían, el sistema se desconectaba dos veces al día, lo cual provocaba que los controladores aéreos tuvieran que salir en desbandada para guiar a los aviones que intentaban aterrizar. Aunque tardaron varios meses, los oficiales acabaron descubriendo que la interrupción la provocaba un

mismo conductor en la New Jersey Turnpike. El individuo utilizaba su interceptor GPS portátil de confianza para evitar pagar peajes en la autopista (y al mismo tiempo paralizaba las pantallas del control del tráfico aéreo[23]). Como es lógico, los interceptores de GPS tienen usos delictivos mucho más graves que evitar pagar peajes en la autopista New Jersey Turnpike. Tras «demasiadas» redadas policiales por sorpresa, tanto la delincuencia organizada como los matones de barrio han aprendido que, si quieres robar un coche, sobre todo con un cargamento lo bastante valioso como para que merezca la pena dotarlo de un dispositivo de seguimiento, será mejor que te facilites la fuga con un interceptor de GPS, y eso es exactamente lo que hacen[24]. La policía de Estados Unidos, Alemania, Rusia e Inglaterra ha visto cómo vehículos robados a los cuales seguían desaparecían de sus radares cuando los delincuentes activaban sus interceptores de GPS, que les proporcionaban una burbuja de seguridad durante su huida. En un caso en el Reino Unido, una mafia utilizó con éxito interceptores de GPS para robar más de cuarenta tráileres de gran tamaño con un cargamento valorado en más de diez millones de dólares.

Dado el nivel de interrupción que generan los pequeños interceptores de GPS, imagina qué podría conseguirse con un modelo de mayores dimensiones. Por apenas unos cuantos miles de dólares se venden interceptores de radiofrecuencia comerciales en Internet. El despliegue de uno o dos de estos dispositivos alrededor de una gran zona metropolitana podría provocar una interrupción generalizada y la convertiría en una diana fácil para cualquier organización terrorista que quisiera captar la atención mundial. Esta amenaza es lo bastante seria como para que el gobierno estadounidense haya emitido una escalofriante advertencia sobre este asunto: «Debemos concebir y ejecutar un plan conjunto entre diversos organismos con urgencia para contrarrestar el “alarmante” auge de la disponibilidad de interceptores de GPS. […] La amenaza para la seguridad nacional podría ser “devastadora”»[25].

Por supuesto, existe una amenaza más siniestra para el sistema de navegación global que impedir que las señales lleguen a tus pantallas: modificarlas antes de que lo hagan. Los interceptores de GPS no sólo son capaces de bloquear las señales relativas a la localización, sino que los falsificadores de GPS pueden alterar los datos posicionales que recibes. La trama diabólica imaginada en *El mañana nunca muere* en 1997 se ha convertido en una realidad, y los dispositivos de manipulación de GPS también están ampliamente disponibles en Internet, lo cual permite a aquéllos con los medios y la capacidad técnica para hacerlo retransmitir sus propias señales de GPS terrestres falsas. A causa de la débil naturaleza de las señales de GPS, los falsificadores «engañan» a los dispositivos de navegación reemplazando su señales legítimas por otras falsas más potentes. Una vez han conseguido anular la señal, los delincuentes, *hackers*, terroristas y gobiernos pueden hacerse con el control absoluto de cualquier receptor de GPS y conectarlo a un simulador de bajo coste capaz de recrear cualquier ruta deseada en un mapa de Google Earth. La emisión de señales falsas puede enviar a un petrolero hacia un puente o a un convoy militar a territorio

enemigo. Y teniendo en cuenta lo obedientes que se han vuelto los conductores con respecto a sus dispositivos GPS, ¿qué estragos podría causar un ataque masivo con datos falsos contra los conductores de una metrópolis?

Hasta la fecha se han producido diversos ataques de manipulación de GPS alrededor del mundo. Pensemos en el impacto que pueden tener en sólo un sector: el transporte mundial[26]. De acuerdo con Cargo Security International, el robo de cargamento cuesta al sector veinticinco mil millones de dólares al año, y el 90 por ciento de los cargamentos internacionales son ultramarinos. El GPS es un componente esencial para garantizar que los artículos correctos llegan al lugar correcto en el momento correcto. Sin embargo, los sistemas de navegación manipulados podrían dejar una mella importante en la armadura de este acuerdo. Todos los buques de pasajeros y de mercancías en el mar (aproximadamente 400 000 barcos en todo el mundo) utilizan el Sistema de Identificación Automático (SIA) para informar de su posición a los demás barcos y las autoridades portuarias, que pueden ver todos los buques de las cercanías en tiempo real. No obstante, en 2013, las investigaciones en materia de seguridad demostraron que el SIA carecía de controles de seguridad siquiera modestos y que era un sistema vulnerable a ataques de manipulación espectaculares[27]. Un ataque contra estos sistemas podría hacer que todos los petroleros y cruceros se desvanecieran de la vista, colisionaran y quedaran encallados. Puesto que los GPS y dispositivos de navegación son «utilidades invisibles», solemos olvidarnos de que existen…, con lo cual nos ponemos en riesgo. Pese a que en el momento de escribir estas líneas la ubicación exacta del vuelo MH370 de Malaysia Airlines desaparecido sigue siendo un misterio, hay algo claro. Los sistemas de navegación responsables de hacer el seguimiento del vuelo eran completamente inadecuados para esta tarea. La posición importa, y la información para la navegación escasa, incompleta o imprecisa cuesta vidas.

Comprobamos el poder de la manipulación del GPS a mediados de 2013 cuando un yate de ochenta millones de dólares fue secuestrado falsificando las señales de GPS. El superyate de lujo y sesenta y cinco metros de eslora *White Rose of Drachs* navegaba frente a la costa italiana cuando, de repente, empezó a virar hacia la derecha[28]. El barco había realizado un crucero mediterráneo entre Mónaco y Rodas, cuando los piratas informáticos activaron su sistema de falsificación de la caja azul. Enfocaron su dispositivo del tamaño de un maletín hacia los sistemas de navegación del yate y lentamente, de manera imperceptible, empezaron a emitir señales de localización falsas. Al principio, la señal recibida desde aquel faro ficticio era deliberadamente débil. Poco a poco, su resonancia fue aumentando, hasta que acabó por igualar primero y superar después las señales reales de GPS que recibía el *White Rose of Drachs*. Llegados a este punto, los *hackers* tenían el control absoluto del superyate y podían dirigirlo adonde quisieran. En el puente de control no sonaron las alarmas y el capitán continuó creyendo, erróneamente, que seguía al timón de su barco.

Las señales falsas eran indistinguibles de las auténticas y su misión se completó. Pese a que quienes viajaban a bordo notaron que el yate había virado bruscamente, en el interior de la sala de mandos del barco todas las pantallas responsables de su navegación mostraban que avanzaba en línea recta. La manipulación de señales en alta mar se había convertido en una realidad. Por suerte para los pasajeros y para la tripulación del *White Rose of Drachs*, el secuestro de aquel barco no corrió a cargo de piratas somalíes, sino de dos estudiantes doctorados de la Universidad de Texas, Jahshan Bhatti y Ken Pesyna. Ambos trabajaban para el profesor Todd Humphreys, quien desde hace años viene planteando su inquietud acerca de la profunda inseguridad del Sistema de Posicionamiento Global y nuestra dependencia de él[29].

De la misma manera que los delincuentes se han hecho con bloqueadores de señales de GPS para facilitar sus robos y vías de escape, sin duda también utilizarán los *spoofers* o suplantadores de señales para encaminar a camiones de dieciocho ruedas hasta puntos de entrega incorrectos y barcos de mercancías hacia atracaderos erróneos, donde los recibirán bandas de delincuentes disfrazadas de trabajadores felices de descargar los artículos y las mercancías en sus contenedores. Un aparato de GPS manipulado equivale a un atraco con éxito. Si esa idea te parece inverosímil, recuerda la ley de Moore y el iPhone que llevas en el bolsillo. Cuanto más pequeño, más rápido y más barato, más tecnología puede filtrarse a los delincuentes, a menudo mucho antes de que su uso sea generalizado entre la población. El control de las pantallas de navegación de los barcos en el mar, los camiones de mercancías, los vehículos de pasajeros e incluso los aviones permite a los *hackers* proyectar una realidad alterada, indistinguible de la verdad, y les brinda un control sin precedentes en un mundo regido por códigos informáticos y pantallas de todos los tamaños y formas.

Asimismo, nuestra fe inquebrantable en las pantallas está sujeta a manipulaciones nuevas y novedosas, que pueden pasar incluso por falsificar los datos de localización que vemos en las aplicaciones de nuestros teléfonos inteligentes. A principios de 2014, un grupo de alumnos del Technion-Israel Institute of Technology de Israel pirateó la popularísima aplicación de navegación con GPS Waze (adquirida por Google en 2013 por nada más y nada menos que mil millones[30]). La aplicación, que proporciona información sobre el tráfico a tiempo real basada en la comunidad, confía en los usuarios para informar de accidentes, controles policiales y peligros en la carretera como medio de mejorar la circulación rodada. Una vez la abres en el teléfono, las lecturas del GPS del dispositivo informan a la red de Waze de la velocidad a la cual avanza tu vehículo, proporcionando con ello información privilegiada en todo momento sobre el estado de congestión de una ciudad. Por lo general, la aplicación funciona como la seda y representa un auténtico salvavidas en ciudades con un tráfico muy denso (de ahí el precio que Google abonó por su adquisición). Sin embargo, tu pantalla de Waze, como todas las demás, puede caer presa de las garras de los piratas informáticos.

Los alumnos de Technion registraron multitud de usuarios falsos de Waze en el sistema utilizando un programa de *scripts* automatizado que programaron para fingir la existencia de miles de *smartphones* (otro ataque de identidades falsas). Luego conectaron a aquellos usuarios de teléfonos móviles virtuales a otra aplicación que facilitaba coordenadas de GPS falsas al sistema de Waze, de tal modo que todos los usuarios parecían estar moviéndose auténticamente por la ciudad. Por último, aquellos usuarios ficticios enviaron ex profeso miles de informes «afirmando hallarse en un atasco en coordenadas falsas». El resultado: el sistema de Waze reaccionó justo como se suponía que debía hacerlo. Redirigió a miles de usuarios fidedignos para alejarlos del atasco simulado y provocó un auténtico embotellamiento en la ciudad al hacer converger a los inocentes conductores a la misma hora en carreteras previamente despejadas. A escala masiva, tácticas de este tipo podrían provocar el pánico y el caos asociados con cualquier otro atraque delictivo o terrorista. Redirigiendo el tráfico, los piratas informáticos pueden conducir a sus víctimas hasta ellos, si bien unos chinos muy inteligentes probaron una táctica distinta y más excitante.

El ataque del general Tso

En lo que los investigadores denominaron una «campaña de ciberespionaje “coordinada, encubierta y dirigida” contra las principales empresas energéticas occidentales», se cree que unos piratas informáticos chinos robaron «gigabytes de documentos clasificados, incluida información protegida acerca de operaciones de oleoductos y gasoductos, financiación de proyectos y documentos de pujas»[31]. Los atacantes desplegaron una gran variedad de técnicas, si bien en algunos casos las altas medidas de seguridad que aplican algunas petroleras les plantearon serios desafíos. La respuesta de los chinos en tales casos no se limitó a golpear más duro a sus objetivos, sino que desató lo que se conoce como un *watering hole attack* («ataque de abrevadero»). Así llamada en alusión a una maniobra similar que los leones del Serengueti han utilizado durante milenios, esta estrategia permite a los depredadores limitarse a acechar junto a un abrevadero donde saben que beben los animales herbívoros. Cuando llegan cebras, antílopes y gacelas, los leones saltan sobre ellas y matan a su presa sedienta. El equivalente online conlleva infectar una web que los objetivos del *hacker* visitan con frecuencia. Cuando un inocente accede a ella y, con toda su buena fe, hace clic en un enlace o se descarga un archivo, el depredador virtual ya tiene a su presa. La única pregunta es qué sitio web infectar.

Tras supervisar las actividades en línea de su objetivo intencionado (una petrolífera estadounidense anónima), los piratas informáticos detectaron un patrón revelador. A sus presas les encantaba encargar comida de un restaurante concreto

cercano a la sede del gigante energético, un restaurante chino famoso por su delicioso «Pollo del general Tso». De manera que los *hackers* infectaron con un programa malicioso el menú que el restaurante chino tenía colgado en Internet y, cuando los empleados vieron aquel plato en oferta, «sin darse cuenta descargaron el código que proporcionó a los atacantes un trampolín hacia la vasta red informática de la empresa»[32]. El hecho de que el gobierno chino utilizara un menú de un restaurante chino para resucitar el poder de uno de sus generales más temibles es a un tiempo brillante, hilarante y profundamente irónico. Te tranquilizará saber que cuando se inquirió acerca de aquel incidente a Wang Baodong, el portavoz de la embajada china en Washington contestó que «las alegaciones acerca del pirateo chino carecían de fundamento. "China posee leyes muy estrictas contra las actividades de pirateo informático; de hecho, China es también víctima de tales actividades"»[33]. Me pregunto qué habría pensado el general Tso del señor Wang.

Juegos en pantalla: pirateo de infraestructuras básicas por mera diversión y para sembrar el caos

Todos los datos que se nos presentan en pantalla pueden piratearse, no sólo la información de nuestros ordenadores portátiles, iPad o incluso menús chinos. Desde los marcadores en un partido de los Lakers hasta los neones y los teletipos de noticias de Times Square, estamos rodeados de pantallas y todas ellas pueden manipularse, incluso nuestros televisores. En 2013, unos piratas informáticos se hicieron con el control del Sistema de Alerta de Emergencias de Montana y emitieron una alerta a través de la filial de la CBS KRTV[34]. La programación televisiva vespertina se vio repentinamente interrumpida por tres pitidos entrecortados y el largo zumbido sofocado del Sistema de Alerta de Emergencias del país, destinado a advertir a la población de desastres inminentes que engloban desde terremotos hasta huracanes. En este caso, no obstante, la advertencia de Montana notificaba al público: «Las autoridades civiles de su zona advierten que los cuerpos de los muertos se están alzando de sus tumbas y atacando a los vivos». El agorero informante avisaba: «No intenten acercarse ni arrestar a los zombis, pues se consideran sumamente peligrosos». Después de que docenas ciudadanos aterrorizados telefonearan a la policía local, la emisora admitió que aquella alerta no era cosa suya: alguien había pirateado la señal de retransmisión y se había hecho con el control de las ondas hertzianas, lo cual le había permitido atacar pantallas desde la CBS.

Incluso las señales viales cotidianas son pasto para los piratas informáticos. En Rusia, el *hacker* Igor Blinnikov logró hacerse con el control de otra pantalla, una valla publicitaria electrónica de seis por nueve metros en una de las principales

autopistas de Moscú, que manipuló en plena hora punta. Desde su domicilio situado a mil kilómetros de distancia, Blinnikov se infiltró en el servidor de la agencia de publicidad propietaria de aquella valla gigantesca y sustituyó los archivos de vídeo de sus anuncios de vodka y moda de grandes marcas por pornografía de alto voltaje. En respuesta, el «tráfico se paralizó cuando los automovilistas curiosos se detuvieron a devorar con los ojos un clip con contenido sexual explícito publicado por los *hackers* en aquellas pantallas de gran formato» en la carretera de circunvalación Garden, que, casualmente, están junto al Ministerio de Interior[35]. Huelga decir que a las autoridades no les hizo ninguna gracia y condenaron a Blinnikov a seis años de prisión.

Cada vez son más las pantallas de señalización pública que se piratean para mostrar mensajes políticos, racistas incluidos. En el punto álgido de las tensiones en 2012 por el tiroteo de Trayvon Martin en Florida, los ánimos estaban inflamados en todo el país. Y precisamente con aquel caso como telón de fondo, alguien decidió manipular el sistema operativo de una señal vial digital de la carretera interestatal 94 en Dearborn, Michigan, y modificar su mensaje de manera que rezase: «Trayvon es sólo un negro». La señal permaneció a la vista de todos los conductores de la ajetreada autopista durante más de una hora, hasta que los operarios lograron apagar el dispositivo y reiniciarlo[36]. Mensajes incendiarios de esta calaña podrían espolear fácilmente una situación ya de por sí tensa y desbordarla. Mediante la manipulación de lo que vemos en las pantallas, televisiones y vallas publicitarias que nos rodean, los *hackers* pueden provocar diversión, pánico o indignación.

El pirateo de señales viales, retransmisiones de emergencia y señales de GPS es causa de preocupación porque todas ellas forman parte de nuestras infraestructuras de información básicas, «elementos nucleares de una sociedad moderna cuya destrucción o incapacidad tendrían un impacto debilitador en la seguridad nacional, la economía, la sanidad pública o la seguridad de la comunidad». El Departamento de Seguridad Nacional de Estados Unidos incluye entre dichos sectores la energía, la alimentación, la agricultura, la sanidad, el petróleo, el gas, el agua, el transporte, los servicios de emergencia, defensa, los servicios financieros y el sector del transporte. Lo único que tienen en común todos estos sectores fundamentales es su dependencia casi absoluta de las tecnologías informáticas y las pantallas como elementos esenciales para su funcionamiento seguro. Y, tal como hemos visto que sucedió en la central de enriquecimiento nuclear iraní, tales elementos también son vulnerables. Este hecho reviste importancia para prácticamente todos los ciudadanos, tanto los del mundo desarrollado como en vías de desarrollo.

Pese a que las amenazas contra cada sector de infraestructuras básicas son demasiado numerosas para enunciarlas aquí, unos cuantos ejemplos relativos al sector del transporte nos servirán a modo ilustrativo. El tráfico rodado, ferroviario, naval y aéreo se controla mediante pantallas y, prácticamente en cada paso, el sistema puede comprometerse. Pensemos en el transporte aéreo: si incluye en la base de datos de

alerta terrorista un perfil falso de un pasajero, un avión puede ser redirigido en pleno vuelo para realizar un aterrizaje de emergencia o ser escoltado por dos cazas F-16. Incluso el proceso de seguridad para subir a bordo de un avión depende enormemente de las pantallas. Los encargados de la seguridad en el transporte no cachean a todos y cada uno de los pasajeros ni abren todas las maletas. En su lugar, dejan que sea la tecnología quien sobrelleve las cargas más pesadas: máquinas de rayos X exploran el equipaje de mano y someten a los pasajeros a una serie de detectores de metal, escáneres de ondas milimétricas y detectores de radiación de retrodispersión. Sin embargo, en todos estos procedimientos de seguridad hay inherente una capa de tecnología que media y separa a los agentes de seguridad humanos de las cosas y personas que investigan, y esa capa ofrece a los piratas informáticos una oportunidad para hacer su trabajo con consecuencias potencialmente mortales.

Pese a que los escáneres de los aeropuertos se antojan máquinas muy complejas y especializadas, sus funciones de procesamiento esenciales están conectadas y se ejecutan mediante ordenadores PC con programas instalados en un sistema operativo Windows normal y corriente y, como todas las máquinas Windows, son claramente manipulables. En pleno año 2014, muchos de estos dispositivos, como el popular Rapiscan 522B, utilizaban variantes de Windows como Windows 98 o incluso Windows XP, sistemas operativos con relación a los cuales se han documentado miles de vulnerabilidades en materia de seguridad y para los cuales incluso Microsoft ha dejado de emitir actualizaciones[37]. Además, las filas de escáneres de los aeropuertos suelen estar conectadas en red entre sí mediantes cables Ethernet o de manera inalámbrica, por medio de Wi-Fi, dos protocolos que también se vulneran de manera rutinaria. Lo más desconcertante es que las contraseñas de los usuarios de muchos detectores de seguridad de los aeropuertos se «almacenan como texto simple y existen múltiples modos de conectarse al sistema sin tener conocimiento previo de los nombres reales de los usuarios». Incluso en el supuesto de que un pirata informático se decidiera a introducir una cuenta y una contraseña inventadas, tras mostrar un mensaje de error, el sistema de estas máquinas le permitiría iniciar sesión, tal como descubrió el investigador en materia de seguridad Billy Rios en Qualys[38].

Dada la cantidad de vulnerabilidades y ataques de día cero existentes en los programas informáticos subyacentes a estos sistemas, si una máquina de rayos X de un aeropuerto se infectara con *software* malicioso y se colocara encima un *rootkit*, los atacantes se harían con el control absoluto de las imágenes que los guardias de seguridad ven en pantalla. Una maleta de mano que contuviera una bomba o un arma de fuego podría aparecer en pantalla como una maleta de mano con tres trajes y un par de zapatos Bruno Maglis. Las pantallas se interponen entre los guardias de seguridad y la labor que desempeñan y, en este sentido, están sujetas a ataques con intermediario tradicionales. En una configuración de seguridad aeroportuaria típica, un guardia observa las maletas cuando entran en la máquina, donde un segundo guardia las somete a rayos X, mientras que un tercer guardia supervisa la retirada de

las maletas a medida que van saliendo del dispositivo. Al tener segmentadas las responsabilidades de este modo, el primer y tercer guardia podrían ver cómo la maleta de mano entra y sale de la máquina, mientras que al segundo se le presenta una imagen de vídeo de una maleta completamente distinta. Puesto que la persona que ocupa la segunda posición rara vez observa el objeto físico, confía completamente en la representación informática que le presenta la pantalla para determinar si la bolsa pasa o no los filtros de seguridad.

Haciéndose con el control de una estación de monitorización de pantallas de vídeo aeroportuaria, los *hackers* podrían permitir que se pasaran armas sin ser detectadas. Y, aunque la Administración de Seguridad en el Transporte (TSA por sus siglas en inglés) se apresuraría a negar tal posibilidad, Billy Rios y su equipo demostraron que dispositivos como el Rapiscan 522B incorporan de fábrica una función de supervisión que permite a los cuadros altos de la TSA ver y controlar docenas de máquinas en los aeropuertos de todo el país en tiempo real, lo cual afecta lo que los guardias de seguridad observan en sus monitores. Sorprendentemente, desplegando una técnica habitual del pirata informático, Rios consiguió pasar la pantalla de inicio de sesión en la consola de supervisión y hacerse con el control de varias hileras de máquinas de escaneado mediante rayos X.[39]

Ahora bien, ¿por qué molestarse en vulnerar insignificantes máquinas de rayos X de aeropuerto si el objetivo es provocar un desastre de gran magnitud? El sistema de control del tráfico aéreo mundial también depende de pantallas, pantallas que los *hackers* ya han atacado con éxito en numerosas ocasiones. De acuerdo con el inspector general del Departamento de Transporte de Estados Unidos, «Los piratas informáticos han coartado los sistemas de control del tráfico aéreo en Alaska, se han hecho con el control de los servidores de las redes de la Administración Federal de Aviación (FAA por sus siglas en inglés), han robado la información personal de más de 48 000 empleados y exempleados de la FAA y han instalado código malicioso en las redes del tráfico aéreo»[40]. El inspector general «advirtió que la FAA no está bien equipada para identificar las intrusiones en sus sistemas informáticos» y destacó que el organismo «tenía sensores de detección sólo en once de sus 734 instalaciones en todo Estados Unidos»[41]. Además, una auditoría de seguridad de las redes del control del tráfico aéreo de la FAA desveló 763 vulnerabilidades tecnológicas de alto riesgo en el sistema[42].

En Estados Unidos, la FAA invierte miles de millones en la mejora del sistema de control de tráfico aéreo del país. El nuevo sistema, denominado Next Generation Air Transportation System o NextGen, «estará muy automatizado y, en lugar de en radares, utilizará GPS para localizar aviones» (en efecto, el mismo Sistema de Posicionamiento Global vulnerable a ataques de manipulación e interferencia sistémicos[43]). Esta modernización de la FAA permitirá a más aviones, helicópteros e incluso drones volar por nuestros cielos, ya excesivamente abarrotados, mediante una red de sistemas de vigilancia dependiente automática (ADS-B en sus siglas inglesas,

de Automatic Dependent Surveillance-Broadcast), pequeños fragmentos de código informático que cada avión emitirá de manera constante a través de frecuencias de radio para anunciar su identidad y localización en el mundo. Por desgracia, estas señales no están encriptadas ni requieren autenticación. Y, en consecuencia, pueden falsificarse y provocar el caos en las pantallas de los controladores del tráfico aéreo. Si los *hackers* se decidieran a inyectar cien vuelos fantasma adicionales en la pantalla de un controlador, sembrarían el pánico. Si tal ardid se prolongara durante sólo una hora, tendría consecuencias en todo el mundo de la aviación civil y paralizaría el tráfico aéreo mundial. Peor aún, analistas de las fuerzas aéreas publicaron un artículo en *International Journal of Critical Infrastructure Protection* que advertía de fallos sistémicos en la técnica de vigilancia aérea ADS-B que «podrían tener consecuencias desastrosas, incluidas entre ellas confusión, derribamiento de aviones e incluso colisiones entre aeronaves si los aprovechaban los adversarios»[44].

La posibilidad de que unos piratas informáticos se apoderen de las pantallas de los controladores del tráfico aéreo mundial es sin duda una perspectiva aterradora, pero también la manipulación de pantallas más mundanas puede tener consecuencias trascendentales, como, por ejemplo, las pantallas de los sistemas de votación. En la actualidad, incluso las urnas a la antigua usanza están siendo sustituidas por programas informáticos y pantallas táctiles. Si bien amañar los resultados de unas elecciones no es nada nuevo (Sadam Husein y Kim Jong-un consiguieron el cien por cien de la aprobación de los votantes con papeletas), la transición a sistemas completamente digitales crea nuevas oportunidades no sólo de subvertir ordenadores, sino ya la propia democracia[45]. Existen docenas de informes acerca de vulneración de las urnas electrónicas alrededor del mundo.

En Washington, D. C., las autoridades querían facilitar el voto a los ciudadanos y, sobre todo, permitir votar a quienes se hallaban ausentes por estar cumpliendo sus deberes militares. En respuesta a ello, la ciudad invirtió centenares de miles de dólares en un sistema de urnas electrónicas. Con todo, a las autoridades del distrito, con buen criterio, les preocupaba que pudieran amañarse los votos en línea. De ahí que, antes de poner en funcionamiento su sistema, lo colocaran en Internet y desafiaran a los piratas informáticos a vulnerar la integridad de la mecánica de la votación electrónica. En menos de cuarenta y ocho horas, los investigadores de la Universidad de Michigan lograron hacerse con el control pleno del servidor de la Junta Electoral. No sólo demostraron que podían modificar cualquier voto entrante, sino que, además, eran capaces de ver en qué sentido había depositado el voto cada votante y, por consiguiente, quebrar el secretismo del sistema de las urnas de papeletas en el cual se fundamenta la democracia[46]. Una vez el equipo de Michigan consiguió apoderarse de la tecnología de votación del distrito, el recuento total distó mucho de estar reñido: Bender, el robot antihéroe de los dibujos animados *Futurama*, fue elegido presidente del comité escolar por una victoria arrolladora. De hecho, ni siquiera se postulaba, pero fue el exitoso candidato agregado y obtuvo la mayoría de

los votos.

Un dato interesante es que, mientras cotilleaban por los ordenadores que habían vulnerado, el equipo de la Universidad de Michigan encontró a otros *hackers* de Irán, India y China intentado subvertir también el sistema[47]. Como tarjeta de visita comercial e insulto final al mundo de las votaciones electrónicas, los piratas informáticos de Wolverine alteraron el *software* del distrito para que cada vez que los votantes hicieran clic en el botón para enviar su votación, los altavoces de sus ordenadores quedaran bajo su control y resonara por ellos el coro de la Universidad de Michigan cantando su himno. Las autoridades del distrito no supieron que el sistema había sido vulnerado hasta dos días después del ataque, cuando una ciudadana anciana telefoneó al Ayuntamiento para informar de que el proceso de votación online le había resultado más sencillo que acudir a un colegio electoral. Al añadir lo mucho que le había gustado la canción que había sonado después de la votación fue cuando la Junta Electoral supo que tenía un problema. La experiencia del Distrito de Columbia no es única, del mismo modo que la integridad de los sistemas de votación electrónicos de Estados Unidos y alrededor del mundo no son ningún asunto esotérico, sino un tema vital para la propia democracia. Cuando los votos se convierten en electrones grabados en ordenadores, los malhechores tienen la oportunidad de ejercer su influencia.

El problema que supone votar y gestionar el tráfico aéreo mediante pantallas es que los sistemas que ejecutan estas infraestructuras esenciales son absolutamente inseguros. Al adoptarlos en nuestras vidas cotidianas sin reflexionar en las consecuencias a todas luces obvias, cada vez estamos más conectados y nos volvemos más dependientes y vulnerables a los subterfugios, con lo cual nos colocamos en un grave riesgo de padecer catástrofes futuras. Dada la oportunidad que los Estados nación tienen de manipular las infraestructuras de información esenciales de todo un país, no debería sorprender que cada vez lo estén haciendo más en casos de guerra y conflicto armado.

Pantallas de humo y la nebulosa de la guerra

Toda guerra se basa en el engaño.

SUN TZU

Desde los tiempos de Sun Tzu, los ejércitos han confiado en el arte del engaño para obtener ventaja táctica con respecto a sus enemigos. En la Antigua Grecia, ese engaño adoptó la forma de un gran caballo de madera regalado al pueblo de Troya. Durante la Segunda Guerra Mundial, fueron las transmisiones radiofónicas falsas y

los tanques inflables de mentira de la Operación Fortaleza los que apuntaron falsamente la existencia de una invasión aliada en las playas de Calais (Normandía) y permitieron a las tropas estadounidenses y británicas recuperar el continente europeo y derrotar a los nazis. Puesto que en la actualidad los soldados experimentan el mundo a través de las pantallas de sus ordenadores, lo lógico es que esa tecnología de la información se haya convertido en el último campo de batalla durante la guerra. Las pantallas indican a los comandantes de las batallas las ubicaciones de sus aviones, barcos, tanques y tropas. Las pantallas gestionan la logística y las provisiones. Y las pantallas proporcionan información de última hora acerca de los planes, las capacidades y las intenciones del enemigo. No debería sorprender que cada vez se las elija con más frecuencia como medio para intentar engañar y derrotar al enemigo.

En la doctrina militar actual, esta índole de actividades recibe múltiples denominaciones, que van desde operaciones informativas hasta guerra electrónica, operaciones de redes informáticas, guerra de la información u operaciones psicológicas. El objetivo común es «influenciar, interrumpir, corromper o usurpar la toma de decisiones de los adversarios»[48]. En el pasado, esto se conseguía difundiendo rumores falsos o información errónea por el boca a boca entre los adversarios o lanzando panfletos sobre poblaciones civiles con mensajes propagandísticos. En la actualidad, todo se reduce a las pantallas. Las pantallas y las tecnologías de la información son idóneas para engañar. El código es débil y fácil de corromper, lo cual redunda en que estos sistemas sean sumamente vulnerables. Además, en su inmensa mayoría están conectados de una forma u otra a la retícula de información global, lo cual posibilita que se infiltren en ellos enemigos ubicados a miles de kilómetros de distancia. Por último, estas tecnologías forman parte de la infraestructura de información básica de cualquier país, una dependencia que hace que tanto un gobierno como su población sean vulnerables cuando se atacan o debilitan tales sistemas.

Algunos de estos intentos de engaño son muy sencillos. En la batalla entre el gobierno sirio y las fuerzas rebeldes, el sitio web de la agencia de noticias Reuters se manipuló para difundir una noticia falsa que sugería que los rebeldes habían sufrido una tremenda derrota en Alepo, lo cual era falso[49]. Otras pantallas de humo digitales son mucho más sofisticadas, como el supuesto pirateo con éxito de los radares sirios por parte de las Fuerzas de Defensa israelíes previo a un ataque contra una instalación nuclear en construcción en el norte de Siria. Bautizada como Operación Huerto, el ataque aéreo destruyó con éxito un reactor nuclear militar secreto que se estaba construyendo con ayuda de los norcoreanos[50]. La incursión obligó a los israelíes a sobrevolar Siria y adentrarse en las profundidades del territorio del país, hasta cerca de la frontera con Irak. Para realizar tal movimiento sin desencadenar una guerra abierta y hacer que derribaran los aviones de su ejército, los israelíes piratearon las defensas aéreas sirias y cegaron a efectos prácticos al gobierno de Assad frente al

ataque que estaba siendo llevado a cabo. Pese a que había aviones enemigos en ruta hacia su objetivo en el interior de Siria, en las pantallas de las fuerzas aéreas sirias reinaban la paz y la tranquilidad[51]. Las pantallas mostraban una realidad distinta en tierra de la que estaba teniendo lugar en el cielo.

En el mundo de las operaciones informativas son muchos los implicados y quienes perpetran los ataques un día pueden ser víctimas de otros ataques al día siguiente. Así sucedió en el punto álgido del conflicto israelí con Hamás en la Franja de Gaza en enero de 2009. En el interior tanto de Israel como de Gaza, la tensión iba en aumento. En cuanto los israelíes comenzaron a movilizar tropas hacia el sur para una posible incursión en Gaza, centenares de reservistas empezaron a recibir su «Tzav Shmone» o llamada de emergencia para incorporarse al deber tanto por el buzón de voz como por mensajes de texto en sus teléfonos móviles. Las reservas se estaban activando y la situación empezaba a ponerse seria en ambos bandos.

Ahora bien, a muchos soldados israelíes se les ordenó que se personaran no en el frente a lo largo de la frontera meridional con Gaza, sino en el norte del país, en un centro de reclutamiento de las Fuerzas de Defensa de Israel en Haifa. Resultó ser que aquellos Tzav Shmone eran ficticios y es probable que los enviara Hamás[52]. En un momento en el que Israel necesitaba que sus soldados se presentaran a cumplir su deber cerca de Gaza, éstos estaban siendo desviados al norte, porque confiaron en las instrucciones que recibieron en sus pantallas. Sun Tzu habría estado orgulloso. Tanto Israel como Hamás habían orquestado un estado de guerra psicológico electrónico contra el otro y Hamás afirmó ser capaz de enviar setenta mil mensajes en una hora a teléfonos móviles israelíes, demostrando con ello que las herramientas tecnológicas desarrolladas por los Estados nación con el tiempo acaban descentralizándose y cayendo en manos tanto de agentes no estatales como de organizaciones terroristas[53].

Existe otro modo que tanto gobiernos como agentes no estatales emplean para enfrentarse por la supremacía de nuestras pantallas: mediante identidades falsas o títeres. ¿Recuerdas los 140 millones de cuentas de Facebook ficticias? No todas están destinadas a aportar «Me gusta» falsos a Shakira. Resulta que tanto militares como agentes de la inteligencia de todo el mundo han acudido en manada a las redes sociales con el fin de manipular lo que vemos en nuestras pantallas y engañarnos. Se sostiene ampliamente que el gobierno estadounidense emplea de manera generalizada identidades falsas como parte de sus operaciones psicológicas (*psyops*) con el fin de combatir la «ideología y propaganda extremistas»[54]. Ello implica que los estadounidenses monitorizan foros web de yihadistas y cuando «Abdul» clama «muerte a los infieles», el Pentágono puede tener a un «Hasán» virtual en el bolsillo trasero listo para responder con un verso del Corán que ensalce la paz, la misericordia y el entendimiento. Por supuesto, eso no es más que el principio de esa capacidad. También aumentan las identidades falsas y, con miles de títeres bajo control, la influencia y la oportunidad de engañar se multiplican de manera exponencial.

En junio de 2011 se reveló que el Mando Central de Estados Unidos había concedido un contrato de 2,76 millones de dólares a una empresa de California para que creara identidades falsas en Internet, con el fin de manipular conversaciones en línea y difundir puntos de vista proamericanos en las redes sociales. Se requería por contrato que cada una de estas identidades online falsas tuviera una historia personal plausible y hubiera «hasta 50 controladores afincados en Estados Unidos […] capaces de operar las identidades falsas desde sus estaciones de trabajo "sin temor a ser descubiertos por adversarios sofisticados"»[55]. El objetivo último del ejército era crear un tablero de mandos de gestión de identidades en Internet que permitiera a cada soldado humano controlar diez identidades distintas ubicadas alrededor del mundo con el fin de «degradar la narrativa del enemigo». ¡A eso le llamo yo proyección exponencial de la fuerza! Las identidades ficticias hablaban en árabe, farsi, urdu y pashto, cosa que permitía a personal militar estadounidense trabajar las veinticuatro horas del día en la manipulación de conversaciones en Internet. El contrato de las identidades falsas formaba parte de una operación militar mucho más amplia, dotada de un presupuesto de 200 millones de dólares y bautizada con el irónico nombre de Operation Earnest Voice (OEV[*]). La OEV se concibió para Irak, «a modo de arma bélica psicológica contra la presencia en Internet de partidarios de Al Qaeda y […] yihadistas de todo Pakistán, Afganistán y Oriente Próximo»[56].

Una vez el motor del engaño virtual exponencial se ha fabricado, quienes lo hacen funcionar y manejan tienen un poder tremendo de sofocar el disentimiento y «degradar la narrativa» de sus enemigos. Lo único que podría evitar el uso de una herramienta de estas características con fines de represión nacional serían la política pública y la legislación, ambas bastante dúctiles y negociables de por sí. Según Freedom House, una ONG fundada en 1941 para abogar por la democracia y los derechos humanos, al menos veintidós gobiernos del mundo manipulan las redes sociales con fines propagandísticos, incluidos Venezuela, Egipto y Malasia[57].

En Rusia, una investigación encubierta realizada por el diario *St. Petersburg Times* reveló que existen numerosos organismos secretos que contratan a jóvenes «operadores de Internet» expertos en tecnología para publicar en Internet artículos y comentarios favorables al Kremlin y difamar a los líderes de la oposición. Cada operador de Internet recibe aproximadamente 36 dólares por una jornada de ocho horas y se espera que escriba al menos cien publicaciones al día[58]. El presidente ruso, Vladímir Putin, un exteniente coronel de la KGB, es un hombre versado en el arte de la propaganda y se sabe que utiliza un «ejército invisible de propagandistas en las redes sociales» para generar hasta cuarenta comentarios al día en su nombre[59]. Ya hable la prensa internacional o nacional de Rusia acerca de los derechos de los homosexuales o los candidatos de la oposición, ejércitos de identidades falsas se colocan para contraatacar al instante y con contundencia. En reconocimiento por su sobresaliente servicio a la nación, sobre todo durante la «liberación» de Crimea, Putin condecoró a muchos de estos integrantes de las redes sociales con medallas de la

«Orden de Servicio a la Patria»[60].

Por descontado, la operación rusa para modelar lo que la población ve en sus pantallas es irrisoria en comparación con las capacidades desarrolladas por la República Popular de China. De acuerdo con el diario *Beijing News* e informes en los medios estatales, China emplea aproximadamente dos millones de trabajadores propagandísticos en línea para dar forma a la opinión pública en Internet y gestionar la vigilancia de la Red en el territorio nacional[61]. Estos comentaristas cobran por «bombardear las redes sociales con noticias e ideas aprobadas por el Estado»[62]. A principios de 2013, el jefe de la propaganda china, Lu Wei, cuyo título oficial es el de presidente de la Oficina de Información de Internet Estatal, ordenó a sus 2,06 millones de ciudadanos en la red que abrieran cuentas en redes sociales como Weibo, un sitio de microblogs similar a Twitter, con la finalidad de difundir «energía positiva» y encauzar los debates en línea acerca de temas sensibles «en la dirección correcta»[63]. Estos empleados también recibieron formación sobre cómo estructurar los debates en Internet y desviar las conversaciones en torno a temas políticos polémicos, y también acerca de cómo cuestionar el valor de los conceptos de democracia occidentales[64].

En manos de los gobiernos, los usuarios títere con identidades falsas devienen un potente complemento a la censura y la vigilancia de Internet. La censura garantiza que el mayor número de ideas «indeseables» jamás consigan franquear un cortafuegos nacional y, en caso de hacerlo, pueden movilizarse legiones de identidades falsas para socavar cualquier idea que no encaje con las que baraja el poder. En ambos casos, las pantallas se someten a un alto grado de manipulación para garantizar que quienes ocupan el poder permanezcan en él y su autoridad no se vea amenazada por nuevas ideas. Cada día, en todo el mundo, guerras de pantallas tienen lugar mientras gobiernos, corporaciones multinacionales, delincuentes y terroristas bregan por dar forma y controlar lo que vemos en Internet. Lo que sigue es una guerra real pero oculta acerca de la realidad, una guerra destinada a cegarnos e impedirnos ver la verdad. Por desgracia, la situación empeorará a medida que nuevas generaciones de tecnologías aún más potentes inunden Internet y nos separen más que nunca de experimentar una realidad a quien nadie más haya dado forma o en la que nadie más haya mediado.

Control + Alt = engaño

Una de las definiciones de la cordura es la capacidad de distinguir lo real de la irreal. Pronto necesitaremos una nueva definición.

ALVIN TOFFLER

En 1865, el Congreso de Estados Unidos aprobó una legislación que permitía al director de la Casa de la Moneda del país añadir el lema «In God we trust» («En Dios confiamos») a todas las monedas de oro y plata acuñadas para ser puestas en circulación. Aquella frase, originalmente extraída de la cuarta estrofa del himno americano, «The Star-Spangled Banner», se ha convertido desde entonces en el credo oficial de Estados Unidos. Si bien en un nivel espiritual muchos estadounidenses poseen hondas convicciones acerca de su confianza en Dios, desde una perspectiva práctica algo ha cambiado. Es posible que acudan al templo los viernes por la noche o a la iglesia los domingos, pero cada día de sus vidas todos miran pantallas. Se diría que nos hemos transformado en una cultura regida por el credo «En la pantalla confiamos». Si algo aparece en una pantalla, ya sea de un ordenador, iPad, sistema de control industrial, señal vial, dispositivo GPS, instalación de radar o teléfono móvil, de manera innata tendemos a confiar en lo que vemos. No obstante, hemos demostrado con sucesivos ejemplos que todo, desde nuestros amigos en Facebook hasta los números que marcamos en el teléfono móvil, puede alterarse para engañarnos. El problema es que vivimos unas vidas plenamente mediadas por las pantallas y otras tecnologías que, pese a ofrecer aspecto de transparencia, en realidad están programadas, controladas y operadas por otras personas. Y lo que es aún peor: ninguno de nosotros tenemos ni la más remota idea de cómo funciona todo este asunto.

Cada día que pasa nos internamos más en una sociedad «de caja negra», en la que unas cajas mágicas nos proporcionan indicaciones, nos presentan las noticias, ejecutan movimientos bursátiles, realizan llamadas telefónicas, recomiendan restaurantes y nos ponen el conocimiento del mundo en la punta de los dedos. Pero el funcionamiento de esta tecnología mística es completamente opaco al usuario medio. Mientras que a la mayoría de nosotros nos complace no tener que aprender los entresijos de programar con código para realizar una llamada telefónica, acudir a un cajero automático, votar o solicitar que nos pongan frenos ABS en el coche, quienes poseen esos conocimientos nos aventajan sobremanera. Son ellos los que se postulan para dar forma al mundo para las grandes masas plebeyas que prefieren delegar en otros estos asuntos técnicos tan farragosos. En un mundo que cambia de manera exponencial bajo la ley de Moore, quienes consiguen saltársela llevan la batuta.

Tal como se ha indicado en el primer capítulo de este libro, cada vez estamos más conectados y nos volvemos más dependientes y vulnerables. La abrumadora mayoría de nuestros sistemas informativos puede vulnerarse en cuestión de minutos y el número de virus, troyanos y ataques de día cero para aprovechar estas brechas ha aumentado de manera pasmosa. El lapso promedio que transcurre desde que un intruso se infiltra en un sistema hasta que se descubre su pirateo no se mide en minutos, sino en cientos de días. Día sí y día también están penetrando en nuestros sistemas, nos están investigando, nos están espiando, nos están robando y nos están manipulando digitalmente, y la mayoría de nosotros permanecemos felizmente ajenos

a tal amenaza. Bienvenido a la nueva normalidad, un mundo en el que gobiernos, delincuentes, terroristas y *hacktivistas* tienen un plan de ataque para cada pantalla presente en tu vida.

Al final, todo pirateo informático, manipulación de código y modificación de pantalla se reduce a una cuestión fundamental de fiabilidad. La fiabilidad es el elemento nuclear de todos estos debates y, en la actualidad, en nuestro mundo no existe nada parecido a una computación fiable. La seguridad, la privacidad y la fiabilidad de la tecnología se perturban, sabotean y socavan con excesiva facilidad. El meollo de la cuestión es que no tenemos una idea terrenal de qué sucede en el interior de nuestros sistemas, los mismos que empleamos a diario a nivel personal y profesional y que hacen funcionar el mundo. Mientras podemos continuar depositando fielmente nuestra confianza en Dios, colocarla en las pantallas es un craso error y acabaremos arrepintiéndonos de haberlo hecho.

El error de seguridad llamado Heartbleed que saltó a la luz a principios de 2014 es emblemático de los desafíos que afrontamos. En teoría, los algoritmos criptográficos están concebidos para codificar y descodificar en secreto información sensible transferida entre dos partes. Los protocolos de encriptación más comunes en Internet son el Secure Sockets Layer (SSL por sus siglas en inglés o «capa de conexión segura») y el Transport Layer Security (TLS o «seguridad de la capa de transporte»). De hecho, una versión del SSL, conocida como SSL abierto, es la responsable de proteger más de dos tercios del tráfico total de Internet. Incluso aunque desconozcas qué es la criptografía o el SSL, es muy probable que los utilices cada vez que te conectas a tu cuenta bancaria en línea, que compruebas tu correo electrónico o que compras en una tienda virtual. Todos hemos aprendido a buscar el pequeño candado verde en la línea de la dirección del navegador web y a comprobar que estamos en una página HTTPS en lugar de HTTP para garantizar que nuestra conexión a un sitio web determinado sea fiable y segura. El verde indica «adelante, es seguro, está bien»… o al menos eso creíamos.

La revelación más importante del *bug* Heartbleed es que incluso aunque los candados verdes que aparecen en nuestros ordenadores nos indicaran que estábamos protegidos, lo cierto es que no era así. La confianza que habíamos depositado en los candados SSL cerrados que aparecían en las pantallas de nuestros navegadores era indebida. Otro engaño del credo «En la pantalla confiamos». Heartbleed es la vulnerabilidad más relevante y generalizada de la historia de Internet hasta la fecha. Este fallo de programación en las SSL abiertas implicaba que alguien más podía acceder a las claves criptográficas secretas que compartías de manera privada con tu banco o con el servidor de las empresas de redes sociales. Peor aún, el fallo había pasado completamente desapercibido, pese a que existía desde diciembre de 2011. Eso significa que todos los mensajes de chat, correos electrónicos, compras efectuadas a través de Internet, visitas a sitios web y descargas de aplicaciones realizadas durante los pasados años en realidad eran plenamente accesibles para

alguien con el tiempo, la energía y las ganas de descifrarlas.

En torno al 66 por ciento de los sitios web utilizan el protocolo SSL abierto, motivo por el cual millones de páginas de todo el planeta tuvieron que informar a sus usuarios de que había un enorme agujero que permitía a los *hackers* esquivar la encriptación entre los internautas y sus sitios web. Instagram, Pinterest, Facebook, Tumblr, Google, Yahoo!, Etsy, GoDaddy, Foursquare, TurboTax, Flickr, Netflix, YouTube, USAA y Dropbox son sólo algunas de las empresas que se vieron afectadas por este problema[65]. A ellas cabe sumar las más de 150 millones de aplicaciones descargadas en la plataforma de móviles Android, también vulnerables[66]. Por desgracia, no bastaba con cambiar la contraseña para resolver el problema por parte del usuario. Antes de eso, cada uno de estos sitios web necesitaba modificar el *software* de su servidor y actualizar la versión de SSL abierta que utilizaba; de otro modo, cualquier atacante potencial seguiría siendo capaz de descifrar tu nueva contraseña incluso después de cambiarla. Transcurrido un mes completo desde que se anunció el *bug* Heartbleed, centenares de miles de sitios web seguían siendo vulnerables a este fallo masivo en la médula ósea criptográfica que sostiene la mayoría de Internet[67]. Como es lógico, los atacantes no perdieron el tiempo en aprovechar la oportunidad que les brindaba Heartbleed, incluida la NSA, que supuestamente hacía años que conocía esta vulnerabilidad pero la había mantenido en secreto para beneficiarse de las oportunidades que le brindaba[68]. Los delincuentes también participaron en la fiebre del oro que suscitó Heartbleed y perpetraron ataques contra la Canada Revenue Agency (Agencia Tributaria de Canadá) y docenas de sitios web de comercio electrónico de todo el mundo[69].

Supuestamente, las claves criptográficas y los certificados digitales deben proteger nuestros datos online y las tecnologías subyacentes a éstos. Ahora bien, Heartbleed no fue la primera vez en que se subvirtieron con éxito dichos sistemas. En gran medida, las herramientas para hacer nuestro mundo tecnológico más seguro y fiable sencillamente son inexistentes. De ahí que carezcamos de los medios que en tanto que sociedad global necesitamos para adoptar decisiones inteligentes y fiables en un mundo cada vez más confuso. Los seres humanos no leemos directamente los ceros y unos de nuestros discos duros ni pensamos en código binario (al menos, aún no). Utilizamos un sinfín de pantallas y otras máquinas para interpretar esa información en nuestro nombre y, al hacerlo, sacrificamos cualquier esperanza real de entender la verdad más implícita de cualquier cosa. Mientras otras personas puedan interceder en nuestras experiencias digitales y virtuales viviremos en un profundo riesgo de que nos defrauden, ataquen y abusen de nosotros, y ése no parece un cimiento demasiado encomiable sobre el cual construir ninguna civilización futura.

Ahora bien, los mayores desafíos que afrontamos en el mundo regido por el lema «En la pantalla confiamos» no son los problemas del hoy, sino los del mañana. Dadas las implicaciones evidentes de la ley de Moore, el número de pantallas que forman parte de nuestras vidas cotidianas en la actualidad empalidecerá en comparación con

lo que está por venir. Parafraseando al rapero Notorious B. I. G.: «Cuantas más pantallas, más problemas». Habrá pantallas por doquier; las llevaremos en las muñecas, en las gafas, en las lentillas y en la ropa, y los dispositivos denominados «ponibles» se volverán moneda corriente. En nuestros hogares, las mesas de nuestros comedores, los marcos de las fotos y cuadros, los frigoríficos y las lavadoras se transformarán también en pantallas. Mientras nos desplacemos a ocuparnos de nuestros asuntos cotidianos, veremos pantallas en nuestros coches, trenes y en el reposacabezas de cada asiento de cada avión. Los menús en los restaurantes, los espejos en los lavabos de señoras y las paredes tras el urinario en los lavabos de señores nos alumbrarán con información visual. Y no sólo todas las vallas publicitarias serán sustituidas por pantallas, sino que también lo serán paredes de hogares, edificios de oficinas y comercios. Las pantallas de aviso, como las que utilizan los pilotos de cazabombarderos y la realidad aumentada se generalizarán y proyectarán capas y más capas de información virtual en nuestra línea de visión, influyendo de manera continua en nuestra opinión. De hecho, todas las superficies posibles se transformarán en una pantalla interactiva y cada una de ellas servirá como filtro a nuestra realidad y podrán ser fácilmente manipuladas por aquellas personas a quienes permitimos que interpreten el mundo real por nosotros.

Hay fantasmas en los cables, pantallas y bancos de datos de este mundo del siglo XXI en el que vivimos. Mientras lo digital y lo virtual ahogan lo real, nuestras vidas estarán intermediadas por otros, pero ¿a qué coste? La red de información global a la que cada vez estamos más conectados y de la cual cada vez dependemos más es profundamente vulnerable.

Se avecina una tormenta y todos los indicios de un desastre están presentes. El lecho de roca tecnológico sobre el cual estamos edificando el futuro de la humanidad es profundamente inestable y, como un castillo de naipes, puede derribarse en el momento menos pensado. Pese a ello, seguimos avanzando y adoptando tecnologías más nuevas y deslumbrantes, cada una de las cuales promete solucionar un nuevo problema o proporcionar una utilidad concreta. El problema no es que la tecnología sea mala; de hecho, la ciencia y la tecnología encierran la promesa de beneficiar sobremanera a la humanidad. El problema, como hemos visto, es que quienes poseen conocimientos tecnológicos, ya sean delincuentes, terroristas o gobiernos corruptos, pueden utilizarlos para atacar a una porción cada vez más extensa de público general en su detrimento. Y si bien las tecnologías actuales han sido una bendición para los actores ilícitos, empalidecerán en comparación con la amplitud y el alcance del cambio político que se desplegará rápidamente ante nuestros ojos en los años venideros. Pronto toda una plétora de tecnologías exponenciales que ahora se hallan en su más tierna infancia, como la robótica, la inteligencia artificial, la fabricación en 3D y la biología sintética, se cernerán sobre nosotros y con ellas vendrán oportunidades para el peligro concomitantes, que incluso podrían cambiar la vida tal como la conocemos.

A pesar de que los delincuentes han aprovechado las tecnoherramientas disponibles hasta la fecha, lo peor podría estar por llegar. La computación vulnerable e insegura ha abonado el campo de batalla para un mundo futuro repleto de delincuencia e inseguridad social. La tormenta ya se ha formado y el resultado bien podría ser un destino para el cual no estamos en absoluto preparados. Bienvenido al futuro de los delitos.

SEGUNDA PARTE

EL FUTURO DE LOS DELITOS

Capítulo 10

Crimen, S. A.

> El crimen organizado en Estados Unidos genera más de cuarenta mil millones de dólares al año […] [y] gasta muy poco en material de oficina.
>
> WOODY ALLEN

Innovative *Marketing* era una pequeña y prometedora empresa de nueva creación que diseñaba productos de *software* pioneros ajustados a las necesidades de sus clientes. Los jóvenes fundadores de la empresa inscribieron la sede social en Belice debido a su régimen impositivo favorable, un movimiento inteligente que copiaron de las prácticas empresariales de gigantes tecnológicos bien establecidos, como Apple, Google y HP, cada uno de los cuales tiene empresas subsidiarias inteligentemente constituidas en paraísos fiscales de todo el mundo. Para reducir aún más los costes generales, Innovative *Marketing* optó por establecer sus oficinas centrales en Kiev, Ucrania, donde había abundancia de estudiantes licenciados en tecnologías muy competentes con grados avanzados en ciencia informática y matemáticas y era posible contratarlos por una fracción de los salarios ofrecidos en Silicon Valley.

Como cualquier empresa innovadora de tecnologías que se precie, Innovative *Marketing* anunció sus productos en Internet mediante banners publicitarios y pagó para garantizar que su *software* apareciera entre los primeros resultados de los motores de búsquedas. Atrajo nuevos clientes aplicando una técnica concebida, perfeccionada y comprobada por Amazon.com conocida como «*marketing* afiliado»: si un cliente potencial hacía clic en el enlace afiliado, Innovative *Marketing* pagaría al sitio web donde se alojaba dicho enlace una pequeña tasa por presentar el anuncio y, si se generaba una venta real, el afiliado recibiría una tasa referencial porcentual. El sistema beneficiaba a todas las partes: incentivaba a una mano de obra a base de comisiones y encauzaba las ventas de *software* hacia la joven empresa.

Los dos empresarios que fundaron Innovative *Marketing*, el indio Shaileshkumar «Sam» Jain y el sueco Björn Sundin, habían seleccionado con esmero su catálogo de productos informáticos. El dúo decidió concentrar sus energías creativas en diseñar una clase radicalmente nueva de antivirus y *software* de seguridad informática en 2006, justo cuando el mundo empezaba a mostrarse más y más preocupado por las ciberamenazas. Al poco el negocio iba viento en popa y las ventas de los productos de la empresa, entre ellos Malware Destructor, System Defender y Windows AntiSpyware, aumentaban año tras año. En breve, primero centenares, luego miles y luego millones de pedidos de sus productos anegaron las oficinas de la empresa en

Kiev.

Innovative *Marketing*, como tantas otras *start-ups* de éxito, tenía más demanda de la que podían abastecer y bregaba por asimilar su rápida expansión. La empresa no tardó en ocupar tres plantas completas de un espacio de oficinas moderno situado en el número 160 de la calle Severo-Syretskaya, en el floreciente barrio industrial de Kiev. En el interior, docenas de expertos informáticos con gran talento generaban como churros código a un ritmo frenético, mientras los ingenieros extendían clústers de nuevos cables Ethernet y añadían filas y filas de servidores informáticos para intentar abastecer la demanda de los clientes.

En el vestíbulo de las oficinas centrales de Innovative *Marketing*, cada vez más amplias, los trabajadores colgaron un logotipo de vidrio cuadrado y retroiluminado con colores tras el mostrador de recepcionistas, las cuales se dedicaban a contestar al teléfono y dar la bienvenida a los empleados al inicio de la jornada. Tras aquella zona de recepción ultramoderna, los ejecutivos trajinaban estableciendo procesos empresariales e instalando sistemas para proporcionar la estructura corporativa necesaria para que la empresa siguiera creciendo. En breve se fueron añadiendo departamentos, incluidos entre ellos el de desarrollo de *software*, garantía de calidad, finanzas, facturación, *marketing*, recursos humanos, traducción y localización de *software*, investigación y desarrollo, producción, externalización y asistencia técnica. Jain y Sundin, cual padres orgullosos, observaban cómo crecía su bebé.

En un breve lapso, Innovative *Marketing* se había convertido en un éxito colosal, una empresa plurilingüe mundial que funcionaba las veinticuatro horas del día, con más de seiscientos empleados y clientes en sesenta países. A través de sus subsidiarias, externalizaba las funciones de centro de atención telefónica a la India para que se ocuparan de la asistencia técnica y de las solicitudes de atención al cliente en inglés. Los clientes que hablaban en alemán eran atendidos por el personal bilingüe del centro de atención telefónica de Polonia y los clientes francófonos se canalizaban vía VoIP hasta Argelia. El proceso de ventas de *software* de Innovative *Marketing* estaba completamente automatizado y los programas se distribuían online. Los clientes podían adquirir sus productos con un solo clic de ratón: se emitían números de identificación que se enviaban por mensaje de correo electrónico, en los cuales se ofrecían garantías de devolución del dinero por todos los productos vendidos. Innovative *Marketing* se tomaba el servicio de atención al cliente muy en serio y aconsejaba a sus clientes que telefoneaban a sus números 800 que sus llamadas podían ser monitorizadas para garantizar la calidad. De acuerdo con las estadísticas que recopilaban los centros de atención telefónica, más del 95 por ciento de los clientes estaban «satisfechos» con el servicio recibido.

Como todas las empresas innovadoras del sector de la tecnología, Innovative *Marketing* tenía una presencia activa en las redes sociales. Cientos de sus empleados se habían creado un perfil en LinkedIn donde indicaban el puesto que ocupaban y mencionaban su historial laboral. Para contratar al personal especializado que

necesitaba para continuar expandiéndose, Innovative *Marketing* insertaba anuncios de empleo en numerosos sitios web profesionales y utilizaba reclutadores para localizar a sus gestores de proyectos, administradores de UNIX, especialistas en optimización en motores de búsqueda, investigadores, ingenieros técnicos y socios para desarrollo empresarial. Con el fin de gestionar su explosiva expansión, Innovative *Marketing* aplicaba diversas técnicas para abordar temas de recursos humanos habituales en el mundo de las *start-ups*. Ofrecía premios a los mejores comerciales y seleccionaba con esmero a sus empleados del mes.

Para aliviar el estrés provocado por el ritmo frenético de trabajo, Innovative *Marketing* recompensaba a sus empleados con viajes en grupo a *resorts* junto al mar, donde los empleados participaban en ejercicios de construcción de equipo, incluidas carreras, escalada, ejercicios con cuerda y competiciones de *paintball*, todo ello destinado a espolear la moral y la colaboración. En todos los sentidos, Innovative *Marketing* era una empresa fantástica donde trabajar y un negocio con unos beneficios salvajes. No obstante, desde la perspectiva del cliente había un ligero problema.

La situación típica era más o menos como sigue. Mientras los usuarios se hallaban sentados frente a sus teclados, languideciendo en Facebook, respondiendo a un mensaje de correo electrónico o comprobando las cuentas del último trimestre, de repente una ventana emergente grande y roja aparecía en el centro de sus pantallas. En ella se leía: ADVERTENCIA: VIRUS GRAVE DETECTADO. Simultáneamente, los altavoces de los ordenadores empezaban a emitir un gemido, mientras el sonido estridente de una sirena les advertía que algo grave sucedía con su sistema. En un instante, el logotipo de System Defender aparecía en pantalla junto a una enorme lupa que parecía estar escaneando los archivos del disco duro del usuario. Uno a uno, largos y complejos nombres de archivos del sistema pasaban volando en rápida sucesión e iba acumulándose un largo listado de amenazas de *malware* en la parte inferior de la pantalla. Al final, System Defender podía mostrar, por ejemplo, veintitrés virus conocidos, siete gusanos y dieciocho programas de *software* espía junto con el agorero mensaje de advertencia: SU ORDENADOR CORRE UN RIESGO INMINENTE DE FALLO DEL SISTEMA Y PÉRDIDA DE DATOS PERMANENTE. HAGA CLIC AQUÍ PARA ELIMINAR TODAS LAS AMENAZAS.

Mientras la sirena continuaba sonando en el fondo de los altavoces del ordenador, la mayoría de los usuarios decidía actuar como dictaba la lógica, haciendo clic en el botón de «eliminar amenazas» que resplandecía frente a sus ojos. Al hacerlo, se los dirigía a una página de compras del producto System Defender de Innovative *Marketing*, un programa informático que costaba 49 dólares y garantizaba resolver todos los problemas informáticos conocidos. Los pocos locuelos que optaban por ignorar la opción de «eliminar amenazas» y hacían clic en cualquier otro punto de la pantalla descubrían que su ordenador había quedado completamente bloqueado, salvo

por el aborrecible sonido de la sirena. La tecla de Escape (Esc) no funcionaba y quedaban atrapados de manera permanente en una pantalla roja mortal, incapaces de controlar sus máquinas. Los más avezados creían que reiniciar el ordenador podía resolver el problema, pero, al hacerlo, volvían a encontrarse con el sonido estridente de la sirena y la misma pantalla roja de alerta implacable. Abonar aquellos 49 dólares era el único modo de recuperar el acceso a sus ordenadores y datos (también se ofrecía una versión especial con asistencia técnica ilimitada por 79 dólares).

Pero ¿qué era exactamente aquel producto de *software* pionero que Innovative *Marketing* había creado? Se denominaba *crimeware* («*software* delictivo») y era una categoría de producto completamente nueva en el sector del *software*: un programa informático que delinque. El *crimeware*, también conocido como *scareware* («*software* que asusta»), *ransomware* («*software* que solicita un rescate») o falso antivirus, no es más que un programa informático malicioso que juega con el temor del usuario a tener un virus. Nos han entrenado a todos para que estemos al tanto de las alertas antivirus y ejecutemos el *software* de seguridad cuando se detecta algún problema. De ahí que, al ver el mensaje de alerta del error grave del sistema generado por System Defender en la pantalla, usuarios de todo el mundo accionaran el botón «eliminar todas las amenazas». Con un solo «pero»: el mensaje de alerta mostrado no era más que un engaño elaborado de programación, un caso desmadrado de nuestra tendencia a confiar en la pantalla.

Los clientes de Innovative *Marketing* en realidad no tenían ningún virus; lo que había sucedido es que les habían secuestrado los navegadores y sistemas operativos. La imagen gráfica animada que parecía mostrar que se estaba escaneando el ordenador del usuario en busca de virus no era más que una artimaña visual, no muy distinta de cualquier animación de Disney. De hecho, no se llevaba a cabo ningún escaneado del ordenador y los virus y troyanos «detectados» eran meros productos de la imaginación del *software* proyectados de manera convincente en la pantalla. Una vez se tendía la trampa a los usuarios de que pagaran y se descargaran el producto System Defender, el *software* tenía una misión primordial: eliminar el programa antivirus legítimo del usuario y, por consiguiente, dejar el ordenador con puertas traseras abiertas, expuesto a la instalación de otro *software* malicioso y programas de registro de pulsaciones de teclas en el disco duro afectado. Peor aún, los datos de la tarjeta de crédito proporcionados para comprar aquel *software* fantasma se ponían a la venta al mejor postor en el mercado negro. Innovative *Marketing*, al margen de todos sus centros de atención telefónica, sus oficinas resplandecientes y los retiros de sus empleados, no era más que una fachada deslumbrante para una vertiente moderna de la delincuencia organizada.

La empresa logró crear un mercado espectacular para sus productos delictivos utilizando a su propio personal y los equipos de sus afiliados para tender trampas en sitios web legítimos con anuncios infectados por *malware* vendidos a través de empresas fachada subsidiarias. Cuando un usuario ingenuo visitaba por casualidad un

sitio web infectado o hacía clic en el enlace erróneo, se descargaba un pequeño fragmento de *malware* que infectaba su ordenador y brindaba a los programadores de Innovative *Marketing* el acceso que precisaban para mostrar sus convincentes estafas con pantalla roja. Con el tiempo, después de que numerosos ciudadanos denunciaran el caso ante las autoridades en docenas de países, la empresa delictiva fue descubierta y los resultados de la investigación fueron asombrosos. Innovative *Marketing* conservaba en sus oficinas copias de todas las facturas que había emitido a sus clientes de *crimeware* en todo el mundo. Sólo en el año 2009 había procesado 4,5 millones de pedidos de clientes individuales, por un precio de ventas medio de 35 dólares, lo cual arroja un resultado de 180 millones de dólares en ingresos para Innovative *Marketing* en 2009, bastante más que los 106 millones de dólares obtenidos por Twitter dos años más tarde, en 2011. En total, Innovative *Marketing* generó la escandalosa cifra de 500 millones de dólares en ventas mundiales durante el período de tres años en el cual vendió su *crimeware*.

Con el tiempo se demostró que los fundadores de Innovative *Marketing* eligieron ubicar su empresa en Ucrania no sólo porque fuera fácil contratar expertos técnicos, sino porque las autoridades formulaban pocas preguntas y era fácil sobornar a los cuerpos de seguridad para que cooperasen. Allí, los empleados jóvenes, como «Maxim», un exprogramador de Innovative *Marketing* de veinte años, admitían que las bonificaciones frecuentes facilitaban hacer la vista gorda a las implicaciones éticas de la empresa. «Cuando tienes veinte años, no te planteas cuestiones éticas», añadió. Y por lo que respecta a los fundadores de la empresa, los señores Jain y Sundin, están imputados por sus actividades y declarados en busca y captura por el FBI y la Interpol. Pese a ello, consiguieron huir a paraísos fiscales antes de que se los arrestara y su paradero sigue siendo desconocido.

Con sus cientos de millones de dólares acumulados en cuentas bancarias secretas alrededor del mundo, estos emprendedores de Internet consiguieron lo que la mayoría de los empresarios de Silicon Valley sólo se atreven a soñar: una salida exitosa para su *start-up*. Pese a haber dejado de funcionar, Innovative *Marketing* probablemente fuera una de las operaciones delictivas tecnocéntricas más lucrativas de todos los tiempos. Ahora bien, no es ni de lejos la única. Se calcula que unos treinta y cinco millones de ordenadores personales en todo el mundo continúan siendo infectados por estos falsos programas antivirus cada mes y ponen 400 millones de dólares al año en manos de los sindicatos de la ciberdelincuencia mundial que continúan operativos. Bienvenido al mundo de Crimen, S. A.[1]

Los Soprano de Internet

Te has creído el cuento de que «La mafia no paga». ¡No seas estúpido! Eso es

para mequetrefes con estrecheces presupuestarias. No para gente como nosotros.

JAMES CAGNEY en *Ángeles con caras sucias*

La delincuencia es un gran negocio y las Naciones Unidas calculan que las mafias transnacionales recopilan más de dos mil billones de dólares al año en beneficios[2]. El dinero procede del narcotráfico, del robo de propiedad intelectual, del tráfico de personas, de la falsificación de anuncios, de la pornografía infantil, de la usurpación de identidades, del contrabando de animales y, por supuesto, de los ciberdelitos. En total, se cree que la delincuencia organizada representa entre el 15 y el 20 por ciento del PIB mundial[3]. Piensa en las redes sociales más extensas e ilícitas del mundo y en la circulación constante de personas y bienes de contrabando a todo lo ancho y largo del planeta, redes operativas las veinticuatro horas del día, los siete días de la semana. Gracias a Hollywood, a la mayoría nos vienen a la mente gánsteres prototípicos cuando pensamos en la mafia, incluidos jefes mafiosos como Tony Soprano, Vito Corleone y Tony Montana. No obstante, los delincuentes de hoy en día han superado en gran medida las estructuras jerárquicas de tiempos pretéritos en pro de organizaciones corporativas modernas. Los capos, dones y tenientes han sido sustituidos por redes de delincuencia locales, externalizadas, puntuales y *ad hoc* que se organizan rápidamente y vuelven a reformularse para aprovechar cualquier oportunidad ilegal potencial[4].

Los tiempos modernos exigen delitos modernos. Como resultado de ello, los Tony Soprano del mundo han construido y nutrido una competente mano de obra de delincuentes mucho más poderosa, de amplio alcance, generadora de beneficios crecientes y experta en tecnologías. A tal fin, las mafias tradicionales, como la Cosa Nostra (la mafia italiana), la yakuza japonesa o los tríades chinos, así como las mafias rusa y nigeriana, han inaugurado divisiones de ciberdelincuencia para aprovechar los pingües beneficios de bajo riesgo que pone a su disposición un mundo conectado globalmente. La ciberdelincuencia no conoce fronteras y ofrece un anonimato magnífico. Es más, rara vez se llega a juicio, en menos de una milésima del uno por ciento de los casos.

La segunda tendencia principal que ha propiciado la explosión de la delincuencia organizada ha sido la profesionalización de los piratas informáticos. Su *modus operandi* ha cambiado de manera significativa desde los felices años ochenta del siglo XX, cuando la mayoría de los *hackers* se dedicaban a jugar con los sistemas informáticos espoleados por la curiosidad o por el deseo de demostrar sus habilidades técnicas. En cambio, ahora el pirateo informático ya no lo ejercen adolescentes con acné que causan estragos desde el sótano de casa de mamá; de hecho, en la actualidad, más del 40 por ciento de los ciberdelincuentes organizados superan los treinta y cinco años de edad[5]. Hace mucho tiempo, los piratas informáticos que actuaban por cuenta propia llegaron a la conclusión de que podían enriquecerse

vulnerando la tecnología. Así nacieron los ciberdelincuentes como Albert Gonzalez. Se dieron cuenta de que era posible ganarse muy bien la vida colándose de manera ilegal en los sistemas informáticos ajenos. Con el paso del tiempo, se difundió la palabra y al poco los *hackers* de todo el mundo tendieron lazos entre sí y crearon redes clandestinas que les permitían colaborar y competir por los beneficios de sus actos delictivos.

El pirateo informático se convirtió así en una actividad completamente monetizada y se ultimó la sustitución de los piratas informáticos por placer por las bandas de pirateo informático lucrativas. Se fundaron entonces nuevos sindicatos de ciberdelincuencia transnacionales, como la Russian Business Network, ShadowCrew, Superzonda y, por descontado, Innovative *Marketing*, con el fin de aprovechar las oportunidades de amplio espectro que brindaban los delitos de la próxima generación. Y el negocio va viento en popa. Por si la amenaza de que unos piratas informáticos que actúan por cuenta propia te robaran la tarjeta de crédito y unos matones te rompieran las piernas no fuera suficiente, en la actualidad las mafias tradicionales y *hackers* con un talento desbordado han aunado fuerzas y las repercusiones para el público general y para el sector empresarial son nefastas. Si bien históricamente en torno al 80 por ciento de los piratas informáticos trabajaban por cuenta propia, en la actualidad las cifras se han invertido. Según un estudio realizado en 2014 por Rand Corporation, el 80 por ciento de los *hackers* trabajan hoy con un grupo de delincuencia organizada o forman parte de uno[6].

Los descubrimientos de Rand me recuerdan la magnífica escena de la película de la década de 1980 *Cazafantasmas* en la que Bill Murray, Harold Ramis y Dan Aykroyd van armados con «mochilas de protones» para derrotar a los fantasmas que han invadido la ciudad de Nueva York. En un momento dado, Ramis comenta a sus dos coprotagonistas: «Había olvidado deciros algo importante. […] No debéis cruzar los rayos. […] Sería malo». Murray replica: «Tengo un poco liado eso del bien y del mal. ¿Qué entiendes por malo?». Y Ramis le responde: «Intenta imaginar el final de la vida deteniéndose instantáneamente y la explosión a la velocidad de la luz de cada molécula de tu cuerpo…». Y Murray contesta impávido: «Y eso es malo… Vale». Si tomamos prestado ese momento entre Murray y Ramis y lo extrapolamos a nuestra realidad, veremos que nuestros mundos en línea y fuera de línea están convergiendo y «rayos» criminales proverbiales se están cruzando, por lo que nos internamos en la gran era de los delitos digitales. En este nuevo mundo de delincuencia digital, los piratas informáticos y los gánsteres de la vieja escuela han aunado fuerzas y han constituido un «Escuadrón de la Muerte» moderno dedicado a utilizar la tecnología en la medida de lo posible para maximizar su poder y sus beneficios a expensas de ti y de mí.

Esta explotación delictiva de la tecnología en sí misma no es ninguna novedad. Cuando la mayoría de los agentes de policía iban a pie o a caballo, los gánsteres de Chicago empezaron a huir en automóvil. Y cuando el agente de policía medio sacaba

un revólver de seis balas, George «Metralleta» Kelly desenvainaba armas automáticas. Los camellos fueron el primer grupo demográfico, después de los médicos, en utilizar buscapersonas y tuvieron acceso a teléfonos móviles antes de que lo hiciera ningún policía. La tecnología aporta eficacia a la delincuencia, motivo por el cual los delincuentes adoptan enseguida todos los avances tecnológicos.

Los forajidos han demostrado ser especialmente versados en el uso y aprovechamiento de las tecnologías creadas por otros y en su apropiación para sus propios fines, siempre a la caza de nuevas oportunidades. Justo cuando los teléfonos inteligentes con conectividad a Internet empezaban a ponerse de moda, las mafias de México D. F. empezaron a usarlos para realizar sus pesquisas. ¿Qué buscaban? A quién secuestrar, por supuesto. Los ejecutivos adinerados que aterrizaban en el Aeropuerto Internacional de México D. F. constituían una variopinta selección de víctimas de secuestro potenciales, pero los delincuentes se preguntaban qué empresa pagaría un rescate más alto (es decir, cuál tendría un mayor retorno por la inversión) por recuperar a sus empleados. Cosa difícil de saber… hasta que aparecieron los teléfonos inteligentes.

Los equipos de la delincuencia organizada desplegados en el aeropuerto se habían apostado en los vestíbulos de llegada, junto a la recogida de equipaje, donde hileras de choferes vestidos con elegancia esperaban a los empresarios que habían contratado sus servicios. Cada chófer llevaba una gran pancarta con el nombre y la empresa del pasajero esperado: Sr. Smith de la farmacéutica Merck o Sra. Jackson de Goldman Sachs, por poner un par de ejemplos. Las bandas delincuentes que operaban en el aeropuerto utilizaron la información de las pancartas de los choferes para buscar el nombre de los ejecutivos en la aplicación de Google de sus teléfonos móviles y determinar qué cargo ocupaban en la empresa y cuál era su valor neto. Una vez detectado el pez más gordo, los secuestradores se limitaban a acercarse al chófer que sostenía la pancarta más rentable y le pagaban para que se esfumara… ¡o, de lo contrario, se enteraría de lo que valía un peine! Un delincuente sustituía al chófer y sostenía tranquilamente la pancarta que había tomado del chófer real mientras aguardaba a su presa. La trampa estaba tendida y el ejecutivo que había descendido del avión se encaminaba directamente a los brazos del falso chófer, todo porque se había pirateado una «pantalla» de cartón. Varios ejecutivos fueron secuestrados y algunos asesinados mediante esta técnica de investigación con teléfono inteligente[7].

Al margen de cuál sea la innovación técnica, los delincuentes se adaptan rápidamente, ya sea imitando empresas noveles reales en Internet o usando de manera fraudulenta sus servicios. Tomando prestada una página de Uber, la aplicación telefónica para compartir coche que conecta a conductores que buscan pasajeros con posibles clientes, una mujer en el Reino Unido creó su propio servicio de solicitud mediante SMS… ¡de vehículos para darse a la fuga! Tras detectar un nicho de mercado entre delincuentes sin ruedas, Nicole Gibson de Londonderry ideó un servicio que ofrecía «enviar un mensaje a un conductor para escapar» en tiempo real

con el fin de ayudar a los ladrones a fugarse limpiamente con los artículos que habían robado en domicilios y empresas a lo largo de la frontera con Irlanda[8]. En San Francisco, los camellos del Dolores Park empezaron a utilizar Square, un pequeño dispositivo de plástico blanco que se conecta al iPhone y permite a cualquiera aceptar pagos con tarjeta de crédito, lo cual permitía a los clientes modernos que rehuían llevar efectivo encima pagar con tarjeta sus pastillas de éxtasis y marihuana[9]. En Nueva York, las prostitutas, cansadas de las cámaras y de los porteros inquisitivos y descarados de los hoteles más chic de Manhattan han decidido recurrir a Airbnb para alquilar apartamentos para sus citas. Dichas prostitutas se hacen pasar por estudiantes o turistas y los ingenuos neoyorquinos que les alquilan sus apartamentos no tienen ni idea de que sus camas se están utilizando para entretener a múltiples clientes y albergar orgías. Un servicio de acompañantes afirmó que se estaba ahorrando «una fortuna» con el uso de Airbnb. «Es más discreto y mucho más barato que el Waldorf», afirmó una trabajadora sexual de veintiún años[10]. Sea cual sea la tecnología o el servicio de Internet, los delincuentes siempre los adoptan en sus fases iniciales y utilizan de modos innovadores las herramientas de última hora en beneficio propio.

Crimen, S. A.: el organigrama

En la página de inicio del sitio web de Innovative *Marketing*, como en los sitios web de tantas otras empresas en Internet, se incluían dos útiles secciones para los visitantes: «Conócenos» y «Preguntas frecuentes». Quienes clicaban en «Conócenos» descubrían que «Innovative *Marketing* se ha esforzado por desarrollar varios productos que ayudan al consumidor a adaptarse a los cambios que propicia la tecnología». Es una manera de decirlo. Sin ningún género de dudas, si hubieran escrito «Innovative *Marketing* se esfuerza por tangar a personas de todo el mundo engañándolas para que crean que tienen un virus y timándolas para que paguen 49 dólares por eliminar algo que no existe», es probable que muchas menos personas hubieran adquirido su producto. Si bien los grupos de la delincuencia organizada no son claros en cuanto a su estructura real y sus prácticas empresariales, una serie de operaciones encubiertas, fuentes de los cuerpos de seguridad y empresas dedicadas al espionaje y la ciberseguridad han arrojado luz sobre su estructura y organización empresariales, que se exponen a continuación[11].

Lo más sorprendente es que el organigrama de Crimen, S. A. resultaría asombrosamente familiar a cualquiera que trabaje en el mundo empresarial tradicional. Se trata de una mezcla del modelo ideado por Peter Drucker[*] y las prácticas empresariales más punteras que se imparten en las Escuelas de Negocios de

Wharton o Harvard. Si bien existen en la clandestinidad digital elementos que no están meramente motivados por fines lucrativos, como los *hacktivistas*, Crimen, S. A. se dedica, sobre todo, a generar dinero… o valor para el accionariado, si se desea expresar así. Estas empresas delictivas recorren largos trechos para garantizar su sostenibilidad, como ubicarse de manera casi exclusiva en paraísos judiciales, lugares con Gobiernos débiles, regímenes políticos inestables y fuerzas policiales dispuestas a mirar para el otro lado, previo pago de una mordida, claro está. En el seno de estos sindicatos delictivos hay división del trabajo, gestión de la cadena de suministros, jefes de departamento, asesores externos y metas de equipo. Para entender el poder y la profesionalidad de Crimen, S. A., ante todo conviene echar un vistazo a su organigrama con el fin de poder deconstruir la organización delictiva moderna. A continuación se relacionan los papeles y las responsabilidades más frecuentes que se basan en investigaciones clandestinas.

DIRECTOR EJECUTIVO.

El director ejecutivo (CEO por sus siglas en inglés) de cualquier empresa delictiva es responsable de adoptar decisiones y supervisar operaciones. Al igual que los empresarios tradicionales, es a él a quien se le ocurre la «gran idea» y quien aporta el capital inicial para ejecutarla. A menudo suele ser una «persona con don de gentes», está bien conectado con el mundo del hampa y actúa como coordinador, encargado de organizar el equipo correcto de delincuentes para llevar a cabo una tarea. No acostumbra a ser una persona técnica, pero contrata a otros con los conocimientos de programación y pirateo necesarios para llevar a cabo su visión. El director ejecutivo de los delincuentes no se implica en el trabajo sucio del día a día ni participa en ningún ciberataque cuyo rastro pueda conducir hasta él. Establece objetivos y metas para su personal y supervisa la distribución de las ganancias, en especial el reparto de primas. El director ejecutivo cuenta con el respaldo de un equipo de líderes, entre los cuales figuran ejecutivos gerentes de primera línea.

DIRECTOR FINANCIERO.

El director financiero lleva «la métrica» del sindicato de delincuentes, incluida la cantidad de *malware* que se ha vendido, cuántas cuentas bancarias se han pirateado y la contabilidad. Emplea herramientas de procesos empresariales y comerciales, inclusive sistemas de informes financieros y bases de datos para gestionar las cuentas por pagar (a los delincuentes independientes contratados) y las nóminas del personal delincuente. También mantiene una red sofisticada de contactos financieros clandestinos para blanqueo de dinero, es responsable de gestionar las cuentas

mercantiles de la empresa fachada y supervisa las transacciones mundiales en diversas divisas, incluidas las empresas de servicios de pago online que se saltan las reglas de «conoce a tus clientes», como Liberty Reserve.

GERENTE DE SISTEMAS.

El gerente de sistemas (también conocido por sus siglas en inglés, CIO) mantiene la infraestructura informática de Crimen, S. A. zumbando con energía. Se encarga de gestionar los denominados servidores informáticos blindados y no rastreables, así como los contratos con empresas de alojamiento web y proveedoras de servicios en Internet fraudulentas para garantizar que su *crimeware* quede fuera del alcance de las autoridades policiales internacionales. El gerente de sistemas ayuda a mantener bases de datos de «clientes» y ejércitos de *botnets* y es responsable de velar por la seguridad de la información, labor que incluye gestionar las «redes *proxy*» o intermedias que preservan las actividades de sus empleados y garantizan que no se los pueda rastrear. El gerente de sistemas se encarga, además, de encriptar los datos delictivos corporativos para garantizar que ni las autoridades ni organizaciones de pirateo delictivo de la competencia puedan leerlos ni utilizarlos.

DIRECTOR DE MARKETING.

Tal como han constatado las empresas legales, contar con un buen producto a menudo no basta. Los beneficios dependen de la capacidad de una empresa (sea legítima o delictiva) de promocionar de manera efectiva sus bienes y servicios. En este sentido, los directores de *marketing* ayudan a redactar textos publicitarios seductores y los proporcionan a redes de afiliación delictivas para su distribución por la clandestinidad digital.

CUADROS MEDIOS.

Estos mandos operativos suelen reclutarse basándose en amistades de larga duración y lealtades a mafias o de sangre a lo largo de períodos de tiempo prolongados. Son responsables de gestionar la mano de obra delincuente más extensa, además de las redes de mando y control que llevan a cabo las operaciones técnicas delictivas de la organización.

ABEJAS OBRERAS/INFANTERÍA.

Son los soldados de tierra en la guerra de los delitos, el equivalente a los camellos de barrio. Trabajan con otros elementos de Crimen, S. A. distribuyendo *software* malicioso a través de enlaces infectados, archivos PDF y sitios web vulnerados. También descifran los códigos CAPTCHA (esos diseños de palabras garabateados que los seres humanos deben escribir en un cajetín de texto para demostrar que son eso: humanos) y ayudan a colocar extractores de tarjetas de crédito en los comercios al por menor y las placas de recubrimiento en los cajeros automáticos.

DEPARTAMENTO DE INVESTIGACIÓN Y DESARROLLO.

Como sucede con la mayoría de las empresas, la manera de aventajar a la competencia es aplicando una investigación y desarrollo (I+D) punteros, y los sindicatos del crimen no son ninguna excepción. El Departamento de I+D se mantiene siempre en alerta en busca de los últimos fallos en el *software* de los ordenadores de sobremesa, aplicaciones móviles y sistemas en red, oportunidades que el resto de Crimen, S. A. puede transformar en dinero. Además, los equipos de I+D son capaces de gestionar un código personalizado especialmente difícil para poder atacar objetivos o sistemas concretos.

PROGRAMADORES, INGENIEROS Y DESARROLLADORES.

Son los cerebros técnicos de la pandilla de delincuentes y son los ingredientes clave de cualquier empresa delictiva en Internet. Estos cerebritos de la tecnología deben programar el código informático y el *software* que infectarán otros sistemas. Construyen sitios web y escriben el grueso del *crimeware*, *ransomware* y *scareware*, incluidos programas antivirus falsos que luego distribuyen los operativos de la red delictiva. Son las personas que programan los *exploits* y el *malware* que infectan y atacan los sistemas de información mundiales. Por descontado, antes de que su código se ponga en circulación se somete a un estricto control de calidad.

CONTROL DE CALIDAD.

El Departamento de Control de Calidad es clave para el éxito de Crimen, S. A. Garantiza que los *shells* o intérpretes de órdenes criptográficas en los que se oculta el *malware* de los codificadores sean lo bastante buenos como para pasar inadvertidos a los sistemas de seguridad, como los programas antivirus y cortafuegos. Los programadores de este departamento cotejan todo el *crimeware* con las definiciones de antivirus conocidas para asegurarse de que su *software* malicioso no sea detectado

antes de ponerse en circulación. Herramientas como avcheck.ru y Scan4You.net permiten a estos equipos evaluar la posibilidad de detección por parte de dieciocho de los programas antivirus más populares. Y lo más importante, estos modelos antidetección se actualizan a diario y están completamente automatizados. Los encargados de comprobar el control de calidad de los programas informáticos delictivos incluso pueden establecer que se les envíen notificaciones cuando las empresas de seguridad identifican como amenaza algún *malware* previo creado por sus programadores. Estas alertas permiten a los programadores actualizar y modificar rápidamente su *software* malicioso para que vuelva a pasar desapercibido y el negocio continúe viento en popa.

AFILIADOS.

El *marketing* de afiliación, como se ha indicado previamente, goza de gran popularidad y genera unos beneficios increíbles en el mundo en línea. Utilizado de manera habitual por Amazon.com y otras empresas, paga a sus afiliados en función del número de clientes que son capaces de conducir hasta un minorista determinado. Las redes de afiliación son la columna vertebral de las empresas de la ciberdelincuencia y la mayoría de las mejores están en Rusia. Los llamados *partnerkas* trabajan día y noche para encauzar el máximo tráfico posible hasta los sitios web de sus socios fraudulentos. Estos delincuentes de poca monta se encargan de colocar productos, ya sean *software* antivirus falso, pornografía infantil, reproducciones de relojes Rolex o Viagra falsificada. El papel del afiliado consiste en presentar la mercancía de los delincuentes a los clientes desprevenidos. Los *partnerkas* difunden sus programas mediante correo electrónico no deseado (*spam*), foros, comentarios en blogs, redes sociales y mensajes SMS. Crimen, S. A. paga a sus afiliados por clic o por instalación cada vez que se desvía tráfico hacia la empresa delictiva o cuando se descarga *malware* en la máquina de una víctima. Los afiliados activos pueden ganar fácilmente 5000 dólares al día, y algunos recaban hasta 300 000 dólares al mes. En el más puro de los paroxismos, los capos de la delincuencia advierten a sus afiliados en los sitios web clandestinos que «el uso de correo no deseado u otros métodos ilícitos de infección de máquinas queda estrictamente prohibido»[12]. En efecto, Crimen, S. A. también ha adoptado los términos de servicio y contratos de licencia con el usuario final para protegerse y desviar cualquier reclamación de actividad delictiva contra los ejecutivos de primera línea.

ASISTENCIA TÉCNICA.

En ocasiones, ejecutar campañas de *software* malicioso puede ser arduo. De la misma

manera que con frecuencia nos vemos obligados a reiniciar nuestros ordenadores, solicitar ayuda al Departamento de Tecnologías de la Información de la empresa o visitar Best Buy Geek Squad, los delincuentes también precisan hacerlo. De ahí que los sindicatos de la ciberdelincuencia modernos ofrezcan asistencia técnica tanto a sus empleados como a sus afiliados.

DIRECTOR DE RECURSOS HUMANOS.

Para implementar con éxito una campaña delictiva mundial valorada en centenares de millones de dólares, como Innovative *Marketing*, se requieren personas, muchas, muchas personas. El equipo de RR. HH. ayuda a reclutar a los soldados rasos delincuentes y a las abejas obreras necesarias para llevar a cabo las operaciones cotidianas de la empresa ilegal. Establece portales web para ocuparse de la «gestión del capital humano», que incluye desde solicitudes de empleo hasta pagas y beneficios y la formación en línea necesaria para poner en práctica una campaña de infección con *software* malicioso. El director de recursos humanos se encargará de publicar anuncios en la clandestinidad digital para reclutar a afiliados perfectamente conscientes de estar colaborando en una operación delictiva. RR. HH. también recluta a otro tipo de empleados: las denominadas «mulas», que pueden o no saber que trabajan para Crimen, S. A. Los anuncios para mulas prometen ingresos elevados, horarios flexibles y la capacidad de trabajar desde casa, y normalmente se publican en Craigslist o incluso en sitios web de empleos legítimos. El personal de RR. HH. se encarga de contestar a las llamadas recibidas de solicitantes de empleo y no duda en responder a las preguntas sobre beneficios salariales y planes de 401 000 dólares (prometidos tras un primer año de empleo exitoso).

MULAS PARA BLANQUEO DE DINERO.

El blanqueo de las ganancias procedentes de actos delictivos es clave para la expansión de cualquier organización ilícita. Todo el dinero generado, ya sea mediante la venta de narcóticos, la instalación de *scareware* o la usurpación de identidad, debe transformarse debidamente en activos a todas luces legales. A tal fin se reclutan «mulas para blanqueo de dinero» mediante empresas fachada, las cuales ayudan a trasladar el dinero de manera anónima de una cuenta, banco o país a otro. Con toda su ingenuidad, las mulas suelen responder a anuncios de empleos con títulos como «ayudante regional», «representante empresarial» o «reclamación de cuentas pendientes». Se les dice que serán responsables de «procesar los pagos» y se las instruye para que abran dos cuentas con su propio nombre, una para su salario y otra para los fondos que se dedicarán a procesar, normalmente a través de Western Union.

Las mulas, que por lo general reciben entre el tres y el diez por ciento de los fondos que manejan, deben proporcionar una fotocopia de un documento de identidad legal, un requisito empresarial legítimo completamente lógico que facilita a Crimen, S. A. dar con los posibles soplones en fechas posteriores.

Las mulas son el rostro de los ciberdelitos y operan con su nombre verdadero, lo cual implica que tienen una vida útil muy breve. Al poco, la policía llama a sus puertas y es entonces cuando estas amas de casa, estudiantes y desempleados de larga duración que no han tenido problema en hacer la vista gorda y no formular demasiadas preguntas constatan que han participado en un asunto ilegal. Para entonces, el dinero y sus «jefes» —que actuaban bajo seudónimos— hace tiempo que se han esfumado. De acuerdo con un experto en mulas para blanqueo de dinero, la carestía de mulas es el principal cuello de botella que afronta Crimen, S. A. en la actualidad. Colarse en el sistema es fácil; cobrar los cheques es lo difícil. Los expertos calculan que la proporción de credenciales de cuentas robadas a mulas disponibles podría situarse en una exorbitante proporción de mil a uno. En otras palabras, con una capacidad suficiente de mulas y RR. HH., las pérdidas atribuibles a la ciberdelincuencia podrían ser diez mil veces peores[13].

La elegante empresa novel (delictiva)

La estructura de Crimen, S. A., como la de cualquier otra organización tecnocéntrica, no es inmutable, sino que fluye de continuo. En su libro *El método Lean Startup*, Eric Ries analiza los métodos mediante los cuales los empresarios noveles son capaces de crear nuevos productos «bajo condiciones de una incertidumbre extrema». Precisamente, donde destacan los delincuentes es en el ámbito de la incertidumbre, pues nunca saben cuándo tendrá lugar la próxima redada policial o si una banda rival aparecerá en un coche y los tiroteará. Quienes operan al margen de la ley se adaptan e innovan constantemente para superar los obstáculos y satisfacer las últimas demandas del mercado. Construyen, miden y aprenden utilizando analíticas web basadas en datos y llevando una buena contabilidad de sus productos y proveedores. Sin embargo, no todas las actividades delictivas se jerarquizan desde altos mandos hasta abejas obreras; algunas son *ad hoc* y mucho más austeras.

Estas organizaciones ilegales están mucho más en sintonía con el mundo que Tim Ferriss describe en *4-Hour Workweek*, donde propone agilizar las actividades empresariales eliminando los gastos de estructura y sistemas automatizados. Las estructuras organizativas densas y el liderazgo evidente se rehúyen en deferencia de productos y servicios oportunos que, en su mayoría, pueden montarse a demanda. Estos actores en línea clandestinos pueden estar mucho más interesados en el equilibrio de la vida y el trabajo o en el diseño del estilo de vida, lo cual les permite

compaginar delitos y juegos mientras maximizan las oportunidades en ambos campos. Forman una suerte de enjambres, grupos de personas en constante movimiento que aportan sus habilidades específicas a un fin común. Su congregación es a la par efímera y amorfa, lo cual hace que su control resulte sumamente difícil. Una vez ejecutada la tarea delictiva, como por ejemplo el desmantelamiento de un importante intermediario de datos o de un minorista, el grupo se disipa para posteriormente reagruparse con otras personas con el fin de perpetrar el siguiente delito.

Quienes participan en estos enjambres delictivos en Internet en ocasiones forman núcleos, basados en su especialidad criminal[14]. Por ejemplo, un círculo de suplantación de identidad podría formar de manera espontánea un núcleo utilizando los conjuntos de habilidades de múltiples enjambres. Un grupo de agentes con conocimientos técnicos expertos podría responsabilizarse de piratear un sistema de datos empresarial, y el grupo siguiente actuaría como agente intermediario de datos, distribuyendo la información personal sustraída a expertos en falsificación de documentos, que elaborarían permisos de conducción, tarjetas de crédito, cheques y pasaportes con dichos datos. Los enjambres de matones del nivel más bajo que ejecutan los fraudes económicos reales transferirían los fondos recibidos a una red de mulas, que, a su vez, colaborarían con una red de blanqueo de dinero para garantizar que todos los implicados en el delito reciban el pago por los servicios prestados y su parte de los beneficios.

Tanto en los mundos de Crimen, S. A. como de las redes de enjambres de delincuentes, la seguridad operativa es fundamental. El trabajo y las comunicaciones se llevan a cabo de manera remota, y se suprime la necesidad de conocerse en persona. El trabajo se compartimenta y estratifica para garantizar que los participantes del grado inferior no conozcan las verdaderas identidades de los demás implicados en el delito. Los foros sobre pirateo y los canales de comunicaciones clandestinos que existen en Internet funcionan como los principales puntos de presentación, reclutamiento y trama de conspiraciones criminales y permiten al enjambre coordinarse en la medida necesaria para completar el trabajo en proyectos específicos.

Una matriz sofisticada para el delito

> Como fiscal de los Estados Unidos en Manhattan, pocas cosas me preocupan tanto como las ciberamenazas que se ciernen sobre nosotros.
>
> PREET BHARARA, fiscal del Distrito Sur de Nueva York, Estados Unidos

Ya se estructuren los grupos de ciberdelincuentes organizados a modo de empresa, como en el caso de Innovative *Marketing*, o como grupúsculos establecidos de manera más espontánea, hay algo claro: su concepción del negocio y de sus «clientes» es harto sofisticada. Se han apropiado de las últimas estrategias empresariales legítimas y son versados en la gestión de la cadena de suministros, la logística mundial, la financiación creativa, la fabricación «justo a tiempo» o en el momento exacto, la incentivación de la mano de obra y el análisis de las necesidades de los consumidores. El resultado es la empresa ciberdelictiva actual, una organización mundial con servicios plenos, múltiples productos y pingües beneficios capaz de derribar a cualquier persona, empresa o gobierno a su voluntad. Tal como se ha indicado previamente, existen al menos cincuenta organizaciones Crimen, S. A. de esta índole en Internet operativas alrededor del mundo[15].

Yo he comprobado esa sofisticación con mis propios ojos mientras colaboraba con la Interpol y la Policía Federal brasileña en casos relacionados con el robo de tarjetas de crédito en toda Latinoamérica. En las favelas de los alrededores de Río de Janeiro, grupos de ciberdelincuentes organizados vendían programas de *software* en discos de DVD que contenían decenas de miles de números de tarjetas de crédito y datos de usuarios. Aquella *start-up* ilegal vendía sus discos DVD a otros delincuentes, a quienes ofrecía descuentos por la adquisición de grandes lotes. También incluían contratos relacionados con los servicios relativos a su *software*, en los que aseguraban que al menos el 80 por ciento de los números de tarjeta de crédito robados funcionarían o «¡te devolvemos el dinero!». Los brasileños proporcionaban incluso números telefónicos de asistencia técnica para otros delincuentes que intentaban ejecutar el *software* pero topaban con dificultades técnicas: «¿Ha probado a reiniciar el ordenador, señor?».

Algunas organizaciones de Crimen, S. A. utilizan *software* de gestión de relaciones con el cliente (CRM) para rastrear las solicitudes de los clientes y generar lealtad a la marca entre los delincuentes, como ocurrió con la empresa novel artífice del fraude bancario Ciudadela de Troya[16]. Dicho *malware*, una variante del infame troyano Zeus, permitió a los delincuentes sustraer información bancaria, registrar las pulsaciones de teclas de los usuarios e instalar otras formas de *crimeware* en la máquina de las víctimas. Cuando los piratas informáticos de Ciudadela vendieron su *software* dañino a otros delincuentes, lo que pretendían era asegurarse de que sus clientes quedaran satisfechos con el *crimeware* que habían creado. Tomando prestada una página de Marshall Field y Harry Gordon Selfridge, la pandilla de Ciudadela prometía: «Mejoraremos nuestros productos de acuerdo con los deseos de nuestros clientes», y hablaban en serio. Sus desarrolladores crearon una interfaz de usuario de CRM que permitía a otros delincuentes que utilizaban el *malware* bancario de Ciudadela enviar informes de errores, hacer propuestas y votar por la inclusión de nuevas funciones en las versiones posteriores del *software*, e incluso enviar partes de incidencias a los programadores y llevar un seguimiento de éstos. Ofrecían asistencia

técnica mediante mensajería instantánea en ICQ y Jabber, y los partes de incidencias se resolvían puntualmente. Los «fraudempresarios» de Ciudadela incluso montaron una red social para permitir a «gente con una mentalidad afín» que empleaba sus troyanos contra la banca reunirse para debatir «proyectos de interés mutuo», como robarnos a ti y a mí.

Crimen, S. A. puede ser extrañamente razonable y racional y utilizar tácticas de eficacia contrastada para mantener su ventaja competitiva y garantizar la continuidad de su funcionamiento. En la clandestinidad digital, esto implica llevar un seguimiento muy de cerca de la competencia y de las potenciales interrupciones del negocio, sobre todo de los cuerpos de seguridad. Tal como hemos visto previamente, los piratas informáticos con fines delictivos no sólo supervisan las actividades de agentes y organismos policiales relevantes, sino que, además, reúnen información privilegiada de código abierto para desvelar cualquier amenaza a sus impresionantes beneficios. Un grupo de ciberladrones responsables de piratear JetBlue, 7-Eleven, JCPenney y el mercado bursátil Nasdaq creó un sistema de «cuerdas de trampa» para activar alertas precoces que les notificaran cualquier novedad acerca del descubrimiento de sus *exploits*[17]. Específicamente, crearon una serie de alertas de Google con palabras clave escrupulosamente seleccionadas que cubrían a sus víctimas objetivo, de manera que si se publicaba alguna noticia acerca de «ataque informático contra Nasdaq», podían detener sus inversiones y desaparecer antes de que la policía tuviera tiempo de dar con ellos. Los piratas informáticos se han convertido en la nueva Mafia y contribuyen diariamente a la industrialización y profesionalización sin límite de los delitos.

El honor entre ladrones: el código ético de los delincuentes

> Para hacer carrera entre delincuentes, hay que tener reputación de ser honrado.
>
> TERRY PRATCHETT, *Pies de barro*

Para mantener una economía clandestina e ilegal ordenada y operativa, Crimen, S. A. debe observar determinadas reglas. Una de ellas es que existe un código de honor entre los ladrones y que algunos individuos pertenecientes a Crimen, S. A. incluso publican «códigos de conducta» para tranquilizar a otros clientes que operan con fines delictivos. Estos cibermercados negros están perfectamente estructurados y se rigen por sus propias políticas, de tal modo que compradores y vendedores informan unos acerca de otros y validan sus reputaciones recíprocamente. Algunos mercados de la delincuencia digital incluso cuentan con sistemas de puntuación de la reputación

para que otros *hackers* puedan valorar las tarjetas de crédito robadas, los permisos de conducir falsificados y los virus informáticos con entre cero y cinco estrellas, tal como se hace en eBay o iTunes[18].

En el escalón más bajo del mercado delictivo en Internet, resulta más fácil acceder a estos niveles y no es infrecuente que se transgreda el código de honor. Estos individuos se conocen como «destripadores» y fracasan en su misión de entregar bienes o servicios ilegales en torno al 30 por ciento de las veces. Sin embargo, una vez identificados, enseguida se los etiqueta, prohíbe y expulsa del mercado… tal como sucede con un vendedor en eBay o Amazon que no cumple su promesa[19]. Para mitigar estos problemas de confianza, los ciberdelincuentes han establecido oficinas de compensaciones y servicios de fideicomiso similares a los que se utilizan al comprar o vender una casa. Estos intermediarios que tiñen de honestidad sus delitos ayudan a verificar que los productos ilegales o datos robados ofrecidos se entreguen de verdad… y sólo entonces liberan los fondos, tras gravar cada transacción con un cinco por ciento[20].

En los estratos más altos de Crimen, S. A., las nuevas incorporaciones a la ciberclandestinidad se revisan a conciencia y debe haber alguien de confianza que responda por ellas, del mismo modo que los narcotraficantes medran por la cadena trófica. En la esfera de los peces gordos, las violaciones del código de conducta escasean y, de producirse, tienen graves consecuencias. Todas las partes saben que acatar las reglas va en el mejor de sus intereses. Del mismo modo que en la delincuencia organizada es habitual tomar represalias, lo mismo ocurre en la ciberclandestinidad. Pese a que darle una paliza a los competidores y arrojarlos con zapatos de cemento al East River es más una jugada típica de los gánsteres de la vieja escuela, sus equivalentes digitales cuentan igualmente con sus propios métodos desagradables. También ocurren tiroteos digitales desde el coche, como el exterminio de dos días de duración perpetrado por Max Ray Vision (alias Iceman), tristemente célebre por haber probado sus armas del teclado contra la competencia y haberla borrado del mapa. Desde su apartamento en San Francisco, Iceman consiguió hacerse con el control de las bases de datos de información de su competencia delictiva, absorber su contenido y utilizarlo para crear su propio sitio masivo, CardersMarket, que acabó contando con seis mil miembros. Empleando los datos robados a su competencia, CardersMarket amasó más de dos millones de tarjetas de crédito hurtadas y acumuló unos 86 millones de dólares en cargos fraudulentos[21]. Las habilidades técnicas superiores cuentan en el mundo de Crimen, S. A., motivo por el cual los piratas informáticos nunca dejan de estudiar y ampliar sus conocimientos.

Delinque y vencerás

Los *hackers* no nacen, se hacen. Se forman, se financian y aprenden de manera autodidacta gracias a la enorme cantidad de material educativo existente en el mundo digital. Crimen, S. A. es una organización de aprendizaje y en Internet pueden encontrarse tutoriales para toda suerte de acciones, desde esquivar salvapantallas hasta clonar tarjetas de crédito. Los delincuentes tienen acceso a sus propios cursos en línea masivos, donde aprenden a lanzar campañas de *phishing* y *spam*, además de a utilizar kits de vulnerabilidades de *crimeware*. Toda esta formación vendría a componer una suerte de Universidad de la Delincuencia a Distancia, la cual ha acelerado la sofisticación y las habilidades de los piratas informáticos individuales. Un dato interesante es que los tutores de los alumnos, que no son más que otros piratas informáticos, a menudo suman esfuerzos para ayudar a los novatos a aprender las artes de la delincuencia digital. En el mundo de la ciberclandestinidad existen numerosas *wikis* que proporcionan enlaces detallados, ordenados por categorías, sobre cómo piratear todos los dispositivos, aplicaciones, programas informáticos y sistemas operativos que existen.

Por supuesto, no toda la formación en informática ilícita y con ánimos de delinquir tiene lugar en el mundo libre. A menudo consideradas como «escuelas de perfeccionamiento» para los delincuentes, las prisiones ofrecen muy poco en términos de reforma y, en cambio, un largo recorrido en cuanto a obtener una licenciatura en delincuencia. De hecho, un estudio de la Universidad de Ohio demostraba que los «individuos con antecedentes penales obtienen unos ingresos ilegales anuales considerablemente más elevados que quienes tienen el historial limpio, a quienes superan en un promedio adicional de 11 000 dólares conseguidos de manera ilícita»[22]. Tal como la universidad mejora el potencial de ahorro de quienes trabajan en la economía legítima, también lo hace la educación de doctorado impartida tras los barrotes.

De ahí que pueda sorprender que cada vez sean más las cárceles que ofrecen formación en informática y programación a los presos. Si bien tales habilidades pueden ser la clave para forjarse una carrera profesional legítima tras quedar en libertad, también pueden serles útiles para fines ilícitos, incluso mientras están en la cárcel. Tal fue el caso de Nicholas Webber, quien, mientras cumplía condena en la cárcel Her Majesty’s Prison Isis del sur de Londres, utilizó sus conocimientos de informática durante su clase de formación en TI para *hackear* el sistema informático de la penitenciaría[23]. En la prisión de máxima seguridad de San Quentin, en las vecindades del Silicon Valley, incluso se ha creado una incubadora de empresas noveles para los reos con ambiciones empresariales[24]. Con el apoyo de los *tecnorati* de la zona, los presos participan en «días de demostración» y ejecutivos del Silicon Valley evalúan el potencial de las ideas de empresas noveles que exponen. Y pese a que la intención de estos programas es encomiable, desde una perspectiva práctica el tiro podría salir por la culata.

La innovación procedente de la clandestinidad

> Un ingrediente básico de la innovación es la capacidad de desafiar la autoridad y transgredir las reglas.
>
> VIVEK WADHWA

Los delincuentes, forzados a operar fuera de los sistemas legítimos de poder, siempre han demostrado ser expertos en innovar soluciones a problemas difíciles y en pensar de manera diferente. Una y otra vez han desplegado una enorme inventiva en sus prácticas empresariales y en el uso creativo de los recursos[25]. En el relato breve «La cruz azul», G. K. Chesterton lo resumía a la perfección con las siguientes palabras: «El delincuente es el artista creativo; el detective sólo es el crítico». El lado oscuro de esta creatividad se materializa a diario en el mundo de Crimen, S. A. El desafío para el resto de la sociedad es que la innovación tecnológica avanza a un ritmo exponencial y, lo más importante, que la ley de Moore también se aplica en el caso de la delincuencia.

La innovación tecnológica surgida en la clandestinidad prospera y el hervidero mental de los delincuentes empieza a dejar rezagados a las empresas antivirus, los vendedores de tecnología y los cuerpos de seguridad. El pirateo informático ha dejado de ser un área exclusiva de unos cuantos gurús digitales selectos; en su lugar, en la actualidad se ha democratizado y toda la información está disponible en la Universidad de la Delincuencia a Distancia. Los delincuentes actuales no sólo innovan tecnológicamente, sino también en sus modelos de negocio[26]. Crimen, S. A. ha incorporado modelos de suscripción para los servicios de *software* malicioso, ludificación para los miembros del personal y desarrollo de programas de código abierto para troyanos destinados a la banca. Para canalizar las ventas, Crimen, S. A. ofrece a otros delincuentes versiones elementales de herramientas de *software* ilícitas o incluso se las proporciona de manera gratuita[27]. Si sus clientes delincuentes están satisfechos con el producto, pueden pagar más y actualizarse a las versiones completas, una estrategia denominada «tarificación *freemium*»[*].

La ciberdelincuencia organizada ha adoptado de pleno la estrategia de «cola larga» de Chris Anderson y concibe el futuro del negocio de la delincuencia como «robar más por menos»[28]. Mientras que los delincuentes del pasado ansiaban dar «el golpe de su vida» (pensemos en *Ocean's Eleven* o en el diamante de la *Pantera Rosa*), los ciberrufianes actuales pueden recabar pingües beneficios simplemente ejecutando operaciones cada vez más nimias contra el público general. Como veremos en el capítulo siguiente, gran parte de estos microrrobos pueden automatizarse, lo cual conlleva un flujo constante de ingresos reiterados emparejado con un menor riesgo de detención.

Con el fin de motivar a una mano de obra delictiva diversa, Crimen, S. A. ha

concebido una serie de programas de incentivos destinados a mantener el negocio en expansión. Para muchos *hackers*, el dinero no es el único acicate; muchos de ellos disfrutan con la emoción de quebrantar las leyes, con el desafío de derribar un sistema de seguridad sofisticado o con el derecho a fanfarronear que les da subvertir un sistema de estas características. Los miembros de la ciberclandestinidad han creado sitios web donde otros piratas informáticos pueden revisar y puntuar sus incursiones digitales. RankMyHack.com premia con puntos a los mejores de los mejores y utiliza tablas de resultados para diferenciar a los aspirantes de la élite de los piratas informáticos[29].

Los capos de la ciberdelincuencia están al corriente de estas tendencias y han hallado diversos modos de satisfacer las necesidades de reconocimiento, desafío y pertenencia de sus empleados mediante la incorporación de elementos de ludificación en sus actividades delictivas. En Montenegro, la banda artífice del *scareware* KlikVIP dio una fiesta para los instaladores de *software* malicioso más productivos y ofreció un gran maletín lleno de euros al afiliado que infectara el mayor número de máquinas[30]. A principios de 2014, en un esfuerzo por impulsar la innovación y crear nuevas líneas de negocio ilícito, un ejecutivo de Crimen, S. A. de Europa del Este ofreció un Ferrari nuevo al pirata informático que inventara la mejor estafa nueva[31]. La noticia del premio se desveló en un recoveco tenebroso de la clandestinidad digital, en un vídeo de producción profesional que incluía a varias «azafatas» glamurosas en el suelo de la sala de exposición del comerciante. La estrategia de ludificación del jefe dio resultado y recibió una amplia atención entre sus empleados. El Ferrari se reservó para el «empleado del mes» elegido

De proyectos de colaboración abierta a proyectos de delincuencia abierta

De todas las técnicas de innovación empresarial utilizadas por Crimen, S. A., la adoptada de manera más generalizada posiblemente haya sido el *crowdsourcing* o proveimiento participativo, es decir: proyectos de colaboración abierta o pública. Este tipo de proyectos surgieron a modo de herramienta legítima para aprovechar el conocimiento de las multitudes con vistas a resolver complejos desafíos científicos y empresariales. El concepto del proveimiento participativo recibió una amplia atención por primera vez en un artículo que Jeff Howe escribió para *Wired* en 2006[32]. Howe definía el proveimiento participativo como el acto de «externalizar una labor a un grupo amplio e indefinido de personas mediante una convocatoria abierta». Si bien se han documentado centenares de ejemplos de proveimiento participativo con magníficos resultados, estas mismas técnicas pueden manipularse

también para servir a fines delictivos[33].

En YouTube abundan los ejemplos de supuestos desconocidos que empiezan a cantar al unísono de manera repentina, ya sea en el Aeropuerto de Heathrow o en Times Square[34]. Sin embargo, estas *flash mobs* o «multitudes espontáneas» podrían degenerar rápidamente en *flash robs* o «robos espontáneos», como parte de los cuales desconocidos con inclinaciones menos caritativas se reúnen no por amor al arte, sino por amor a delinquir. Pese a que los robos instantáneos suelen ser una herramienta de los matones de pacotilla, lo cierto es que tienen una buena tasa de éxito. En Washington, D. C., treinta adultos jóvenes se coordinaron mediante las redes sociales y mensajes SMS para entrar a toda prisa en una tienda de G-Star Raw y huir de ella con prendas de ropa valoradas en 20 000 dólares, aprovechando su superioridad numérica con respecto a los dependientes[35]. Si uno de los participantes implicados hubiera sido arrestado, probablemente no sería capaz de delatar el nombre de sus conspiradores, a quienes habría visto por primera vez en la escena del delito. Incidentes similares han tenido lugar en Chicago, Filadelfia y Los Ángeles.

Algunas técnicas de proveimiento participativo están concebidas para otorgar ventaja a los delincuentes frente a la policía. En Estados Unidos, aplicaciones para móviles como DUI Dodger, Buzzed y Checkpoint Wingman permiten a quienes han bebido demasiado conocer mediante la recopilación de fuentes la localización de los controles de alcoholemia, verlos en un mapa interactivo en un dispositivo iPhone o Android y recibir alertas cuando dichos controles se cambian de lugar o se instalan de nuevo[36]. Cuando las protestas de 2011 en Londres contra los recortes en gasto público del gobierno estallaron en violencia, los manifestantes crearon una aplicación llamada Sukey, que les permitía fotografiar a la policía y cargar sus imágenes geoetiquetadas en un mapa interactivo generado por convocatoria abierta[37]. Cuando otros manifestantes abrían Sukey en sus móviles, sabían en qué áreas se estaban registrando cargas policiales y unas brújulas interactivas en pantalla les asesoraban de cómo evitar a la policía (el verde señalaba las zonas seguras y el rojo las zonas peligrosas con presencia policial).

También los *hacktivistas* han aprovechado las técnicas del proveimiento participativo. En el punto álgido de su disputa con Sony y News Corp, LulzSec tuvo la desfachatez de establecer una línea de atención telefónica para solicitudes de delincuentes en la cual los *hacktivistas* podían solicitar quién debía ser su siguiente objetivo[38]. El grupo registró un número telefónico en Ohio y grabó un mensaje de bienvenida con acento francés que advertía a quienes llamaban: «Lo sentimos. En estos momentos no estamos disponibles porque estamos expoliando Internet» y les solicitaban que dejaran sus peticiones de *hackeo* después de sonar el pitido[39]. Este nuevo *modus operandi* en la recaudación de delitos permitía al público votar quién debería ser la próxima víctima, como si se tratara de un programa al estilo de *Operación Triunfo*. El grupo publicó posteriormente una declaración en la que

afirmaba que había perpetrado con éxito ataques DDoS contra ocho de los sitios web sugeridos por las personas que les habían telefoneado. El proveimiento participativo de delitos puede definirse como la adopción de un delito en parte o en todo y su externalización a una multitud de personas, ya sean o no conscientes de estar participando de él. Mediante la adopción agresiva de técnicas de proveimiento participativo, Crimen, S. A. consigue construir redes delictivas distribuidas en la mayor parte de los casos de manera anónima, las cuales son capaces de organizarse por sí mismas a una velocidad asombrosa. Para poner estas capacidades en perspectiva, en 2013, los jefes de Crimen, S. A. en Rusia y Ucrania fueron capaces de soltar a cien mulas para lavado de dinero en un hospital del estado de Washington que habían pirateado. El ataque se saldó con el robo de más de un millón de dólares del sistema de nóminas del hospital y el blanqueo del capital a través de noventa y seis cuentas distintas en cuestión de pocos días[40]. Tal como se ha indicado previamente, muchas de estas mulas podrían haberse incorporado sin saberlo a este grupo organizado, convencidas de estar «trabajando desde casa» como «representantes regionales de las cuentas por pagar».

La tecnología facilita como nunca a Crimen, S. A. la capacidad de distribuir su trabajo entre multitud de compinches involuntarios que desconocen que están participando en un plan ilegal. A título de ejemplo, los delincuentes necesitan un flujo constante de cuentas de correo electrónico nuevas desde las cuales enviar sus ataques de correo no deseado y *phishing*, pero los CAPTCHA pueden ralentizarlos. Para salvar este obstáculo, concibieron un *software* que tomaba automáticamente la imagen del CAPTCHA que aparecía en Yahoo! o Hotmail y la enviaba a desconocidos al azar para que la teclearan por ellos. Pero ¿por qué un completo desconocido iba a ayudarnos? Muy sencillo. Se les incentivaba adecuadamente… con pornografía[41]. Para distribuir este problema, Crimen, S. A. creó docenas de sitios web pornográficos gratuitos e informaba a sus visitantes de que tenían que introducir un CAPTCHA para demostrar que tenían más de dieciocho años y poder acceder a ellos. No obstante, el acertijo que el público calenturiento estaba introduciendo en realidad era el CAPTCHA que los delincuentes necesitaban para crear sus cuentas de correo electrónico para el envío de *spam*, CAPTCHA que se cortaba, pegaba e intercambiaba en tiempo real. Generaron así una situación donde todos ganan: porno de alta calidad gratuito a cambio de participar sin saberlo en el envío de correos de *phishing* a gran escala.

Mas, por muy ingeniosa que pueda parecer esta argucia de los CAPTCHA, se queda en mantillas en comparación con la convocatoria de *casting* para delincuentes publicada en un anuncio en Internet. En Seattle, Washington, un atracador de bancos había determinado de manera escrupulosa el día y la hora a los que estaba programado que un camión blindado entregara una gran suma de dinero en efectivo en la sucursal local de Bank of America. Aquel martes en cuestión, a las once en punto de la mañana, el ladrón, con un chaleco de seguridad amarillo, gafas de

protección, una camisa de obrero azul, un cinturón de herramientas, un casco de obra y una máscara respiratoria puestos se acercó a pie al guarda del camión blindado mientras éste transportaba varias sacas grandes de dinero al banco y le roció la cara con espray de pimienta. El guarda, incapacitado, dejó caer las bolsas de dinero, que el ladrón metió en una gran bolsa de lona antes de escapar con lo que la policía de Monroe describió como «una gran suma de dinero»[42]. Cuando el guarda recobró la compostura y lanzó una llamada de socorro a través de la radio y dio la descripción del ladrón, media docena de coches patrulla encendieron las luces y las sirenas y se dirigieron a la escena del delito, en busca de un obrero de la construcción que acababa de dar su gran golpe[43].

El primer coche patrulla que apareció en escena vio al obrero de la construcción, de manera que los policías le apuntaron con sus armas y le ordenaron que pusiera las manos en alto y se arrodillara. Luego otro coche patrulla divisó al obrero de la construcción culpable, y luego a otro obrero y a otro obrero más. De hecho, había docenas de obreros de la construcción en la escena que encajaban con la descripción proporcionada por el guardia del camión blindado. Lo que las autoridades no entendieron inicialmente era que el ladrón del banco real había orquestado con sumo cuidado su huida con antelación. Pocos días antes del robo, el ladrón había colocado un anuncio en la sección de solicitud de ayuda de Craigslist, supuestamente para buscar a obreros de construcción y formar un equipo de mantenimiento de carreteras. Con un salario estupendo, de cerca de 30 dólares por hora, se requería a los interesados que se personaran el martes a las once de la mañana en la intersección donde se hallaba el Bank of America. Ah, y también se les pedía que trajeran su propio equipamiento, en concreto: chaleco de seguridad amarillo, gafas de protección, una camisa de trabajo azul, un cinturón de herramientas, un casco de obra y una máscara respiratoria. Docenas de hombres en busca de aquel empleo se personaron en el lugar y a la hora designados, ajenos a que, sin querer, estaban participando en un atraco a un banco con recursos externalizados. En el mundo gobernado por el lema «En la pantalla confiamos», es fácil engañar al público. Sólo cuando los obreros de la construcción se vieron rodeados y fueron detenidos, la policía cayó en la cuenta de lo sucedido; por descontado, para entonces, el ladrón de verdad se había esfumado.

Crimen, S. A. no sólo está adoptando rápidamente formas voluntarias e involuntarias de externalizar o distribuir sus delitos, sino que, además, utiliza otra tendencia candente en la comunidad de las empresas noveles: el *crowfunding* o micromecenazgo. El micromecenazgo es un proceso mediante el cual se recaudan pequeñas aportaciones de multitud de personas que respaldan bien una empresa novel, bien un proyecto no lucrativo, los cuales se describen con todo lujo de detalles en un sitio web. Los sitios web más populares de esta especie son Kickstarter e Indiegogo, y decenas de miles de proyectos se han financiado de manera exitosa, recaudando más de mil millones de dólares entre la población general[44]. Por

supuesto, los delincuentes están más que dispuestos a atacar informáticamente a cualquiera que consiga amasar tal suma de dinero y ya han conseguido poner en jaque la web de Kickstarter[45]. Al margen de ello, los piratas informáticos malhechores tienen en mente planes de micromecenazgo de una envergadura y una vileza muy superiores, como infiltrarse en el iPhone que llevas en el bolsillo. Cuando Apple lanzó al mercado su teléfono móvil iPhone 5S, incluía una característica conocida como Touch ID, un escáner de reconocimiento de huellas dactilares vendido como «un modo práctico y altamente seguro de acceder a tu teléfono». Aunque probablemente Apple hubiera invertido varios años y millones de dólares en desarrollar su tecnología biométrica patentada, al introducir aquella funcionalidad, en realidad lo que la empresa hizo fue lanzar un guante desafiando a los piratas informáticos a vulnerar tal «sistema altamente seguro».

En todo el mundo, profesionales de la seguridad y piratas informáticos por igual se preguntaban quién sería el primero en vulnerar lo invulnerable y cuánto tiempo tardaría en conseguir hacerlo. La respuesta fue el Chaos Computer Club de Alemania y tardó un solo día[46]. Utilizando elementos tanto de micromecenazgo como de ludificación, los piratas informáticos establecieron un sitio web llamado IsTouchIDHackedYet.com, ofrecían una recompensa de 20 000 dólares, aportada por otros *hackers*, y utilizaban un tablero de puntuaciones para mostrar quién se acercaba más al premio[47]. Al final, éste recayó en un pirata informático conocido como Starbug del Chaos Computer Club, quien en un alarde de ingenio logró subvertir la inversión multimillonaria de Apple. Starbug tomó una fotografía a la altísima resolución de 2400 dpi de las manchas de aceite de las huellas dactilares dejadas en la pantalla de inicio de Touch ID por el dueño legítimo del dispositivo. A continuación, importó la imagen en Photoshop, la limpió, la invirtió y la imprimió en una película transparente utilizando un ajuste de tóner denso. Por último, roció cola para madera blanca de calidad sobre el patrón y, cuando se hubo secado, pudo sostener la huella dactilar ficticia sobre el sensor de Touch ID para desbloquear el teléfono[48]. Misión cumplida.

Por si el micromecenazgo delictivo no fuera ya bastante grave, recientemente ha aflorado otra empresa de proveimiento participativo en la clandestinidad digital: Assassination Market («Mercado de Asesinatos»). Por desgracia, el servicio no es ninguna broma de muy mal gusto, sino la labor de un anarquista consagrado que opera bajo el seudónimo de Kuwabatake Sanjuro. A fecha de finales de 2014, ocho funcionarios del gobierno de Estados Unidos han sido seleccionados mediante un proceso de proveimiento participativo para ser asesinados, y, entre ellos, el expresidente de la Reserva Federal, Ben Bernanke, ha recibido el mayor número de votaciones. Las donaciones se han efectuado mediante divisas online encriptadas y no rastreables, y Sanjuro ha recaudado mediante este proceso de micromecenazgo 75 000 dólares que entregará al asesino a sueldo que se cobre la vida de Bernanke[49].

Ahora bien, por mucho que la recaudación de 75 000 dólares resulte alarmante, ni

siquiera se acerca de lejos al ejercicio de micromecenazgo criminal más exitoso de todos los tiempos, uno en el que ni las víctimas ni el público financiaron la actividad de manera voluntaria. En el que tal vez sea el mayor golpe maestro perpetrado hasta la fecha por Crimen, S. A., ladrones de todo el mundo externalizaron un robo en veintisiete países distintos perpetrado de manera simultánea en todos ellos. Aquel latrocinio masivo tuvo lugar a principios de 2013, cuando programadores, ingenieros y el equipo de I+D de Crimen, S. A. en la Europa del Este se infiltraron en la red de dos procesadores de tarjetas de crédito de la India y una de los Emiratos Árabes Unidos. Crimen, S. A. robó números de tarjetas de débito MasterCard y Visa prepagados y luego se coló en los sistemas informáticos internos de los procesadores para eliminar el límite de crédito de las tarjetas que habían sustraído. Como resultado de ello, aquellos avezados *hackers* contaron con centenares de tarjetas de débito, cada una de ellas capaz de retirar fondos ilimitados de la red de cajeros automáticos mundial[50].

Crimen, S. A. envió a continuación mensajes encriptados a través de la clandestinidad digital a socios delincuentes en más de dos docenas de países. Quienes recibían los datos hurtados usaron sus propias estampadoras de tarjetas de crédito profesionales e ilegales para imprimir las tarjetas de débito y codificar los números de éstas en las bandas magnéticas del reverso. Lo que sucedió a continuación tal vez pueda considerarse uno de los mayores hitos en la historia de la externalización de los delitos, e incluso del micromecenazgo. Las tarjetas se distribuyeron entre centenares de equipos de delincuentes rasos en todo el mundo. Cuando Crimen, S. A. dio la señal, se desató la carrera y la infantería de delincuentes se lanzó en una parranda de retirada de dinero sincronizada contra tantos cajeros automáticos como fue humanamente posible. En el lapso de diez horas que duró la operación de proveimiento participativo de Crimen, S. A., los ladrones realizaron treinta y seis mil transacciones en cajeros automáticos de veintisiete países y arramblaron con más de cuarenta y cinco millones de dólares en efectivo. Puesto que Crimen, S. A. había secuestrado previamente los ordenadores de los bancos y tenía los números de tarjeta de crédito que éstos habían asignado, pudieron contemplar exactamente cuánto dinero se estaba extrayendo y, lo que es más importante, determinar cuánto tenía que abonar cada delincuente base antes de cobrar por «sus servicios». Pese a que un puñado de matones de medio pelo cayeron en manos de la policía, los cerebros de Crimen, S. A. que idearon aquel plan siguen estando sin identificar y probablemente en estos momentos se estén dedicando a organizar su próxima broma de proveimiento participativo a gran escala. Diez horas, treinta y seis mil transacciones, veintisiete países: toda una proeza logística que pocas empresas o gobiernos podrían ejecutar. Bienvenido al mundo de la delincuencia distribuida en red.

Crimen, S. A. es un negocio muy provechoso. Ajeno a la responsabilidad y consideraciones morales, es libre de aprovecharse sin límite y emplear las últimas prácticas del sector para hacerlo. Crimen, S. A. utiliza tarificaciones *freemium*,

ludificación, proveimiento participativo, micromecenazgo, motores de reputación, fabricación justo a tiempo, formación en línea y grupos de gestión de proyectos distribuidos en busca de la larga cola de víctimas de delitos alrededor del mundo. Los sindicatos de delincuentes mundiales, como Innovative *Marketing* en Kiev, han acumulado más de quinientos millones de dólares (libres de impuestos, claro está) en sólo tres años. Estas personas que operan al margen de la ley, estos forajidos de la ley de Moore, están conectados en red y son capaces de utilizar y subvertir cualquier tecnología a su antojo. Lo hacen con casi total impunidad y sus acciones ponen en peligro a un mundo cada vez más conectado y profundamente dependiente de la tecnología para funcionar. El resultado es una clandestinidad delictiva cada vez más potente cuyas capacidades se multiplican de manera exponencial. Este superorganismo delictivo floreciente vive, respira y está controlado desde los recovecos más profundos y oscuros de Internet: la Internet Profunda (también conocida como Internet Invisible o Dark Web), el sanctasanctórum de la clandestinidad digital y el centro neurálgico de Crimen, S. A.

Capítulo 11

Viaje al centro de la clandestinidad digital

> La representación del delincuente estándar se fundamenta en los atributos de las personas menos inteligentes a quienes atraparon.
>
> NASSIM NICHOLAS TALEB, *El cisne negro*

Dread Pirate Roberts (DPR) era el hombre más buscado en la clandestinidad digital. Desde las profundidades más abisales del ciberespacio, el misterioso delincuente regentaba un imperio inmenso de operaciones ilegales encubiertas. Era objeto de una caza humana mundial, perseguido de manera activa por agentes especiales del FBI, la Administración para el Control de Drogas (DEA por sus siglas en inglés: Drug Enforcement Agency), el Departamento de Alcohol, Tabaco, Armas de Fuego y Explosivos (ATF por sus siglas en inglés), el Departamento de Seguridad Nacional de Estados Unidos, la Policía Real Montada del Canadá, Scotland Yard y la Interpol. Apenas se sabía nada de él, salvo que había tomado su alias de un personaje de la película clásica de culto *La princesa prometida*. DPR era el cerebro tras Silk Road, un mercado negro en línea minuciosamente oculto de la vista pública en el que podían adquirirse toda suerte de artículos ilícitos a través de una web secreta: «Si se fuma, se inyecta o se esnifa, hay muchas posibilidades de que la encuentres en Silk Road»[1].

Bautizada en honor a la antigua ruta comercial asiática, Silk Road («la Ruta de la Seda») era un lugar donde comprador y vendedor podían reunirse de forma anónima para intercambiar bienes y servicios en un emporio de contrabando de una envergadura abrumadora. Conocida como la «eBay de las drogas y el vicio», Silk Road ofrecía todos los productos ilícitos imaginables, perfectamente clasificados por categorías como armas o drogas, cada uno de ellos acompañado de fotografías y una descripción. Entre otros artículos a la venta figuraban cuentas bancarias robadas, divisas falsificadas, AK-47, munición antiblindaje, tarjetas de crédito robadas, virus informáticos, registradores de pulsaciones de teclas, cuentas de Facebook vulneradas, tutoriales sobre cómo piratear cajeros automáticos, pornografía infantil e incluso asesinos a sueldo. Bajo la categoría de falsificaciones había más de doscientos listados de permisos de conducir, pasaportes, cartillas de la Seguridad Social, facturas de servicios, extractos de tarjetas de crédito, diplomas y otros documentos identificativos falsos.

No obstante, en su esencia, Silk Road se fundamentaba en el tráfico de drogas, con más de trece mil publicaciones de sustancias controladas a la venta listadas. La

«narcocopia» de mercancías incluía: heroína, oxicontina, cocaína y *crack*, morfina, LSD, éxtasis, pastillas, marihuana, *crystal meth*, setas, jeringuillas, precursores, esteroides, estimulantes y una panoplia de pastillas con receta médica, desde Adderall hasta Xanax. Los narcóticos se vendían tanto en cantidades para consumo propio como en grandes volúmenes, y había ofertas por la adquisición de varios kilos de heroína, cocaína y metanfetaminas. Al hacer clic en un enlace concreto aparecía una imagen del producto en cuestión, así como un eslogan publicitario descriptivo del estilo de «HEROÍNA Black Tar de Nod: dulzura directa a las venas… o a los pulmones si prefieres fumártela y cazar al dragón»[2].

Durante casi tres años, Dread Pirate Roberts manejó el mercado negro en Internet más extenso del mundo y atrajo a más de 950 000 usuarios a crear cuentas en Silk Road. Pero ¿cómo era posible que una violación tan flagrante de la ley operase durante un período tan prolongado sin que se produjera ninguna intervención policial productiva? Muy sencillo: la policía no tenía ni idea de cómo detenerlo. Silk Road no era un sitio web estándar, accesible a todo el mundo con sólo teclear www seguido de algo en la barra de dirección del navegador. Por el contrario, funcionaba en la clandestinidad digital, oculta bajo capas y capas de secretismo proporcionado por un *software* especializado de encriptación y ofuscación conocido como The Onion Router o por su abreviatura: Tor (lo analizaremos más adelante). Utilizando el *software* Tor, todas las partes que compraban y vendían bienes ilícitos podían mantener el anonimato y sólo se identificaban mediante el nombre de pantalla inventado que hubieran elegido. Para proteger aún más a los usuarios y sus actividades ilegales, la única forma de pago aceptada en Silk Road era bitcoin, un nuevo tipo de moneda electrónica que permitía a todas las partes intercambiar fondos online con un altísimo grado de protección de la privacidad.

Los expertos consideraban asombrosamente certera la referencia frecuente a Silk Road como una eBay de las drogas. En sintonía con las últimas técnicas de Crimen, S. A., DPR instituyó un sistema de reputación online robusto que permitía a los usuarios evaluarse y otorgarse confianza mutua antes de efectuar ninguna transacción. Así es, se puede puntuar al camello personal. De este modo, Basehead888 podía ver que DealioInThe312 había realizado más de 4600 ventas de cocaína y había obtenido un 97 por ciento de aprobación de los clientes entre sus devotos seguidores colocados. Los comentarios específicos dejados por los clientes destacaban «la rapidez del envío» y «la solidez del paquete furtivo: ni un perro detector de drogas lo encontraría».

Con el paso del tiempo, la popularidad e infamia de Silk Road iba en aumento y al cabo de poco se intercambiaban cerca de 600 000 mensajes privados mensuales entre compradores y vendedores. Al final, el volumen de tráfico y las transacciones aumentaron de tal manera que DPR era incapaz de gestionarlas por sí solo. En respuesta a ello, este capo de la mafia contrató a un reducido personal de administradores de sistemas que recibían entre mil y dos mil dólares mensuales por

mantener el sitio web operativo en el día a día. Entre sus tareas figuraban supervisar la actividad de los usuarios para detectar posibles problemas, proporcionar atención al cliente y actuar como mediadores cuando existía alguna disputa entre un comprador y un vendedor. Por descontado, el fundador del mayor mercado de la droga ilegal y clandestino del mundo ganaba unas sumas significativamente superiores a las de sus empleados, cosa que los administradores de sistemas de rango inferior no tardaron en averiguar. Para subsanar la injusticia percibida de un salario bajo, uno de los empleados de Silk Road empezó a desfalcar a la empresa. Y como sabe cualquiera que haya visto *El precio del poder*, *Los Soprano* o *El Padrino*, robarle al capo no es buena idea.

Cuando Dread Pirate Roberts constató que le estaban desfalcando, fue incapaz de tolerar la traición, de manera que contrató a uno de los muchos asesinos a sueldo que se anunciaban en su sitio web y negoció pagar 80 000 dólares por que le dieran una paliza mortal al empleado (el 50 por ciento por anticipado, de acuerdo con el código de conducta estándar de los asesinos). DPR se sentía tan ultrajado por la falta de respeto que había demostrado su empleado que dio instrucciones específicas al sicario de que torturara al que pronto sería su exadministrador de sistemas antes de matarlo. DPR envió al asesino la dirección de su empleado en Utah y accedió a pagar el resto de lo acordado tras recibir una prueba fotográfica del asesinato. Días más tarde, el director ejecutivo de Silk Road recibió la verificación que había estado esperando en forma de fotografía JPEG. Hombre de palabra, DPR transfirió los 40 000 dólares restantes al asesino e incluso adjuntó una nota de agradecimiento, lamentando, en un mensaje de correo electrónico encriptado: «Me disgusta haberlo tenido que matar […] pero lo que está hecho, hecho está […]. No atino a entender cómo pudo ser tan estúpido […] Ojalá hubiera más gente íntegra en el mundo». Como lo oyes: al fundador de Silk Road, el mayor mercado negro del mundo, al hombre que acababa de encargar a un sicario que matara a su propio empleado, le molestaba la falta de integridad en el mundo.

Con todo, aquélla no era la primera vez que Dread Pirate Roberts ordenaba matar a alguien que lo había traicionado. Sus abusos eran un secreto a voces en la clandestinidad digital e incluso el Senado estadounidense celebró audiencias en las que solicitaba que se emprendieran acciones policiales. Por supuesto, el FBI y otros organismos ya se estaban ocupando del caso y habían concluido más de cien compras encubiertas en el sitio web. Al poco se hallaban tras la pista del padrino de Silk Road, el emprendedor, asesino y señor de la droga en Internet que lo había ideado todo. La cacería humana mundial de Dread Pirate Roberts acabó conduciendo a los cuerpos especiales del FBI dedicados a Silk Road hasta la sucursal de la Biblioteca Pública de San Francisco en Glen Park.

Allí, un día frío y soleado de otoño de 2013, un hombre que rozaba la treintena, con el cabello castaño ondulado, acomodó su ordenador portátil en la tranquila sección de ciencia ficción y empezó a teclear mientras otros usuarios a su alrededor

leían libros y hojeaban revistas. De súbito, una muchacha rompió el silencio y se abalanzó sobre él gritando: «¡Me tienes harta!». En un instante, estaba encima de él y le había arrebatado el portátil. Mientras él luchaba por recuperar su ordenador, los otros usuarios de su mesa, en lugar de ayudarlo, lo arrojaron contra la pared y permitieron a aquella extraña que se fugara con su posesión más preciada.

No fue un robo al azar. Muchos de aquellos supuestos bibliófilos habían aguardado pacientemente a aquel joven y su portátil. En cuanto el joven encendió la máquina e introdujo todas las contraseñas necesarias para desencriptar el disco duro del ordenador, los asaltantes saltaron sobre él. El enfrentamiento acabó en un instante, cuando los supuestos ladrones metieron sus manos bajo sus camisas y, uno a uno, fueron sacando sus placas doradas del FBI. Los bibliotecarios, desconcertados y boquiabiertos, observaron cómo aquel joven con el cabello ondulado era arrestado y conducido a la prisión de Glenn Dyer en Oakland. El «temible pirata Roberts» había dejado de serlo.

Pese a que DPR se había esforzado por proteger su identidad utilizando Tor y bitcoin para cubrir sus huellas, había cometido una serie de errores operativos de novato que acabaron revelando al FBI que solía conectarse a Internet desde la Biblioteca Pública de San Francisco. De acuerdo con la presentación de cargos federal, Dread Pirate Roberts en realidad se llamaba Ross William Ulbricht, tenía veintinueve años y era originario de Texas, si bien se había trasladado a San Francisco varios años antes.

El fiscal de Estados Unidos para el Distrito Sur de Nueva York acusó a Ulbricht, alias DPR, de diversos delitos, incluidos entre ellos «conspiración para cometer narcotráfico, pirateo informático, blanqueo de dinero y regencia de una empresa delictiva». Ah, sí, desde luego, Ulbricht también fue acusado de intento de homicidio y de «usar las instalaciones comerciales interestatales para cometer asesinatos a sueldo». Resulta que el sicario profesional a quien DPR creía haber contratado en realidad era un agente federal de incógnito. Los abogados de la acusación presentaron contra Ulbricht cargos por encargar un total de cinco asesinatos adicionales. Cuando Ulbricht había pagado las sumas exigidas por el supuesto asesino, el FBI supo que iba en serio e intervino para salvar a sus objetivos. Dichas personas accedieron a cooperar con el FBI, que pudo tomar fotografías escenificadas de las supuestas víctimas cubiertas de sangre falsa y con maquillaje facial grisáceo, de aspecto cadavérico, fotografías que enviaron a DPR como prueba de los asesinatos que había solicitado.

¿Quién era aquel cerebro de la delincuencia al mando de Silk Road? Alguien muy distinto a quien cualquiera habría imaginado. Ross Ulbricht era el hijo del que todo padre se sentiría orgulloso, un explorador con rango de Eagle Scout de Austin, Texas, licenciado en Ciencia e Ingeniería. En la escuela de posgrado, Ulbricht había acabado perdiendo el interés en la ciencia a favor de una nueva pasión por el libertarismo. En su perfil de LinkedIn había escrito que ahora deseaba «utilizar la teoría económica

para abolir el uso generalizado y sistémico de la fuerza por parte de las instituciones y el gobierno en contra de la humanidad». A tal fin dio vida a Dread Pirate Roberts y la Silk Road de Internet se convirtió en el lienzo sobre el cual pudo poner a prueba y perfeccionar los límites de sus ideales del mercado libre. El resultado, como le ocurre en la ficción a Walter White en la serie televisiva *Breaking Bad*, fue la historia real de un científico que convirtió su pasión por las drogas y el criptoanarquismo en el mayor proveedor online de contrabando de la historia. Y en el proceso, ese antagonista hizo dinero, mucho, mucho dinero.

Al igual que eBay, Silk Road cargaba una comisión por cada transacción, de entre un ocho y un quince por ciento en función del tamaño de la venta. Sorprendentemente, de acuerdo con los cargos presentados contra Ulbricht, Silk Road procesó más de 1200 millones de dólares en transacciones sólo entre febrero y julio de 2013, lo cual reportó unos ingresos netos a su joven fundador de veintinueve años de ochenta millones de dólares en comisiones. Nada mal para una empresa novel de dos años de existencia. En el punto álgido de su funcionamiento, según un estudio publicado en el diario *Addiction*, cerca del 20 por ciento de los consumidores de drogas de Estados Unidos habían adquirido narcóticos en Silk Road.

Ulbricht fue declarado no culpable de todos los cargos y sus amigos y familiares lo han descrito rotundamente como «un tipo agradable» e incluso lanzaron una campaña de micromecenazgo para ayudar a pagar las costas procesales (en la que se aceptaban bitcoins, claro está). En cambio, el gobierno federal pintó una imagen mucho más perturbadora de Ulbricht en su formulación de cargos, describiéndolo como un señor de la droga, asesino a sangre fría y cerebro criminal perturbado que reinventó por completo el modelo de negocio de Crimen, S. A. Explorador o villano, hay algo inequívoco: Ulbricht, alias Dread Pirate Roberts, ha añadido un nuevo seudónimo a su larga lista de nombres, el del reo ULW981, que permanece confinado en una celda veinte horas al día y afronta una cadena perpetua[3]. Entre tanto, como una Hidra multicaule, Silk Road, que permaneció cerrada sólo brevemente, vuelve a hervir de actividad, bajo una nueva dirección, y florece y se propaga por las vastas extensiones de la Internet Profunda que es la clandestinidad digital.

Pasaporte a la Internet Profunda

Para que los compradores y vendedores ilegales de Dread Pirate Roberts pudieran efectuar transacciones en su mercado de Silk Road, primero tenían que averiguar cómo adentrarse en él. Como sucede en el mundo real, uno no consigue un kilo de metanfetamina llamando a la puerta de una casa cualquiera de un edificio. Y lo mismo ocurre con la clandestinidad digital. No basta con escribir la dirección en el navegador Firefox para ser transportado como por arte de magia al sanctasanctórum

de Crimen, S. A. Se necesita un pasaporte y un *sherpa* que te guíe. Este viaje comienza con Tor (The Onion Router), una herramienta de *software* que proporciona lo más parecido al anonimato real en Internet[4].

Tor funciona encaminando las conexiones web a través de un despliegue mundial de cinco mil servidores informáticos cuyo cometido es ocultar el origen y el destino de la conexión. Sin Tor, tus actividades en Internet son fáciles de rastrear y cada vez que visitas sitios web como CNN o ESPN.com, revelas tu localización y la red de tu casa. Y eso es algo que a los delincuentes no les gusta, porque sería muy fácil atraparlos. De manera que, en lugar de ello, ocultan y canalizan su tráfico mediante servicios como Tor. De este modo, la policía no puede ver que los gánsteres están vendiendo AK-47 online mediante el servidor Comcast en Chicago (a un mero apercibimiento de distancia de identificar al cliente de Comcast al cual se asignó la dirección del protocolo de Internet en cuestión). En su lugar, cualquier pirata informático con experiencia, pongamos por caso afincado en Moscú, canalizará su tráfico de Internet a través de Londres, Ciudad del Cabo, Tokio, Austin y Milán, antes de saltar de la nada y atacar un objetivo en Manhattan. Y así, esa «llamada» proverbial resulta casi imposible de rastrear.

Mientras que el cliente de *software* de Tor puede utilizarse para visitar de manera anónima cualquier sitio web habitual, como Google, su verdadera potencia radica en el hecho de permitir conexiones con servicios ocultos de Tor, a saber: sitios web específicamente configurados para recibir sólo comunicaciones entrantes a través de la red de Tor. Sin el cliente de *software* Tor, es imposible acceder al inmenso contenido oculto en la red de The Onion Router. Con los servicios ocultos de Tor, el visitante del sitio no sólo preserva su privacidad, sino que también tiene la posibilidad de visitar cualquier sitio web clandestino. En lugar de utilizar una dirección web estándar como Facebook.com, todos los servicios ocultos de Tor tienen sus propios nombres de dominio, que acaban con el sufijo «onion». Este sistema de doble anonimato permite tanto al comprador como al vendedor de Silk Road realizar transacciones visitando un único dominio oculto (en el caso de Silk Road: silkroadvb5piz3r.onion) sin revelarse nunca sus verdaderas identidades mutuamente.

Pese a que la mayoría de las personas nunca lo han visto ni lo han utilizado, el *software* de Tor puede descargarse de manera gratuita a través del sitio web de Tor, www.torproject.org. Se instala en cuestión de minutos y, ejecutando el programa con sigilo, transporta a los usuarios fuera del camino trillado de la red de información global general. Curiosamente, Tor se creó y financió en un origen como proyecto del Laboratorio de Investigación Naval de Estados Unidos en 2004, con el respaldo de la Electronic Frontier Foundation y el Departamento de Estado, para ayudar a los disidentes políticos de ultramar y a los activistas defensores de la democracia a organizarse y comunicarse entre sí de manera segura. Tor tiene varios usos completamente legítimos y quienes se encuentran tras los grandes cortafuegos de China, Irán y otros lugares del planeta dependen de él de manera rutinaria para

acceder a cualquier cosa, desde Facebook hasta el *New York Times*. Además, cada vez lo utilizan más los periodistas para comunicarse de manera segura con sus fuentes e informantes, por ejemplo los que operan dentro de la comunidad de WikiLeaks.

Con todo, aunque es posible que Tor se creara para bien, dada su potente habilidad de facilitar las comunicaciones clandestinas no sorprende que los delincuentes hayan adoptado esta herramienta en manada, lo cual ha posibilitado la creación de servicios como Silk Road. Si bien es difícil hacer cómputos exactos, un estudio de cuarenta mil sitios Tor ocultos realizado en 2013 reveló que casi el 50 por ciento de ellos estaban involucrados en actividades ilícitas, como vender tarjetas de crédito robadas, cuentas pirateadas, armas, drogas y pornografía infantil[5]. Algunos expertos en seguridad y cuerpos policiales calculan extraoficialmente que hasta el 85 por ciento de los servicios ocultos de Tor podrían ser ilegales, pues la tasa de adopción de este *software* entre delincuentes supera con creces la de los activistas de la privacidad.

A principios de 2014, el *software* de Tor se había descargado cerca de ciento cincuenta millones de veces y lo utilizan unos dos millones de personas a diario[6]. Si damos por válida la cifra más conservadora del 50 por ciento de uso ilícito, ello implica que cada día 300 000 delincuentes se levantan y van a trabajar en la clandestinidad digital empleando los servicios ocultos de Tor. Según la ley de Metcalfe, el valor de una red de telecomunicaciones es proporcional a la raíz cuadrada del número de usuarios conectados al sistema y, en este sentido, la amenaza procedente de una población activa delictiva, anónima y totalmente conectada en red es enorme.

Crimen, S. A. podría no ser la única fuerza tenebrosa que utiliza Tor para acceder a servicios web ocultos. Varios informes destacan que Al Qaeda y sus filiales también aprovechan el secretismo y el anonimato que proporcionan los protocolos de encriptación de Tor para comunicarse, reclutar a nuevos miembros, recaudar fondos, difundir propaganda e incluso planificar operaciones[7]. Después de que el extrabajador independiente para la NSA Edward Snowden filtrara detalles de las inmensas capacidades de interceptación de las comunicaciones del organismo para el cual trabajaba, aparecieron pruebas que sugerían que numerosos grupos terroristas habían replanteado sus estrategias de comunicaciones y en numerosas misivas recalcaban a sus integrantes la importancia creciente de realizar movimientos seguros en Internet[8].

Organizaciones como Al Qaeda en la península Arábiga y Ansar al-Mujahideen incluso han producido materiales de formación y vídeos de YouTube instando a sus miembros a utilizar Tor para todas sus actividades en Internet[9].

Habida cuenta de las revelaciones de Snowden, así como de los asaltos generalizados contra la privacidad previamente descritos, sería absolutamente lógico que los ciudadanos corrientes empezaran a utilizar una herramienta como Tor para mantener su dignidad, libertad y derechos humanos en Internet. Dicho esto, los

servicios ocultos de Tor han sido completamente usurpados por Crimen, S. A. y la innovación que han liberado y que continúan liberando en la clandestinidad digital es alucinante tanto por lo que respecta a sus dimensiones como a su alcance y escala.

Viaje al abismo

Internet es un expendedor automático para los estados mentales patológicos.

PHILLIP ADAMS, presentador
y escritor australiano

Si pensabas que sabías cómo funcionaba Internet, te equivocas. Matas el tiempo a diario viendo vídeos en YouTube, actualizando tu estado en Facebook y comprando en Amazon, convencido de que te encuentras en un Jardín del Edén sin fronteras en línea, pero no es así. Desde la primerísima vez que te aventuraste a conectarte a Internet, tan sólo has visitado la Red superficial. Has quedado atrapado en un jardín amurallado, cuidadosamente manipulado y podado sólo para ti mientras que los verdaderos expertos se han internado en Matrix, el otro mundo en línea. Ésta es la Internet que la mayoría de nosotros nunca verá. Recibe multitud de nombres: la Internet Profunda, la Internet Invisible, la Internet Secreta, la Deep Web o Dark Web y la clandestinidad digital, por citar sólo unos cuantos. Es la Internet a la sombra, y Google desde luego no te va a conducir a ella.

Técnicamente, la Internet Profunda alude a los recursos informativos en línea que motores de búsqueda como Google, Yahoo! y Bing no pueden indexar, bien porque están protegidos mediante contraseña, bien porque se encuentran tras pasarelas de pago o bien porque requieren *software* especial para acceder a ellos. Dado que el sofisticado *web crawler* o rastreador de la Red que Google utiliza para buscar todo el contenido de Internet no está capacitado para teclear, no puede introducir contraseñas, rellenar CAPTCHA ni registrarse en sitios privados y, por consiguiente, nunca cataloga grandes fragmentos de la información mundial. Gran parte del material no indexado de la Internet Profunda se encuentra en bases de datos académicas como LexisNexis o en conjuntos de datos de actualidad como los que albergan la Oficina de Patentes o la Oficina del Censo. Sin embargo, además del material mundano, también hay material mucho más salaz.

Te sorprenderá saber que la Internet Profunda es quinientas veces más grande que la Red superficial que utilizas cada día para efectuar tus búsquedas[10]. Mientras que la Internet Profunda contiene siete mil quinientos terabytes de información, el universo *googleable* alberga unos irrisorios diecinueve terabytes. Según un estudio publicado en *Nature*, Google no capta más que el 16 por ciento de la Red superficial y queda al margen de toda la Internet Profunda[11]. En consecuencia, cuando efectúas

una búsqueda en Google, sólo ves el 0,03 por ciento (una de tres mil páginas) de la información que existe realmente y que estaría disponible en Internet si supieras cómo acceder a ella[12]. En otras palabras, una búsqueda en Google se salta el 99 por ciento de los datos de la World Wide Web[13]. Buscar en Internet hoy en día es como pescar en el medio metro superior de los océanos más extensos del mundo. Aunque es posible que pesques algún pez en la red, te pierdes la monumental munificencia que existe justo bajo esa capa, en la inmensidad de los mares[14]. Para los intrépidos, hay un equivalente digital a la Fosa de las Marianas, una verdadera cueva del tesoro de datos sin descubrir a la espera de ser explorada.

Como una muñeca *matrioska* rusa, albergado en el interior de esa Internet Profunda hay otro mundo oculto, una comunidad más reducida pero significativa en la que los malhechores aúnan fuerzas para delinquir. Bienvenido a la Red Oscura, una inmensa clandestinidad digital en el seno de la Internet Profunda donde *hackers*, gánsteres, terroristas y pedófilos desempeñan su actividad. La Red Oscura alberga algunos de los secretos más relevantes de Internet y, como los callejones traseros y los bazares del mercado negro de cualquier gran ciudad, es en ella donde los delincuentes entran en contacto para llevar a cabo sus actividades ilícitas. La Red Oscura utiliza encriptación y canales de transmisión en Internet entre pares específicamente diseñados para ocultar las direcciones IP de sus usuarios y, por consiguiente, ofrece una plataforma anónima, no rastreable y segura para que Crimen, S. A. se comunique y haga negocios sin temor a la injerencia del gobierno o el mundo empresarial.

Pese a que Tor es la puerta principal y más popular a la Red Oscura, tiene competencia, como Freenet y I2P (el Proyecto de la Internet Invisible). Más aún, Silk Road es sólo uno de los supermercados de delincuencia online; otros son: Black Market Reloaded, OpenMarket, Sheep Marketplace, Agora, BlackBank, Atlantis y Pirate Market, y nuevos canales se añaden y suprimen a diario. Es importante que los delincuentes, como cualquier empresario que se precie, aprendan de sus errores del pasado y, como tal, en la estela del desarme de Silk Road ha surgido una nueva generación de bazares en la Red Oscura que vienen a llenar su vacío, el más destacable de los cuales es DarkMarket. Mientras que el control de Silk Road estaba centralizado en las manos de DPR y los servidores informáticos que éste administraba, DarkMarket es un mercado negro en línea completamente descentralizado y sin un dueño único[15]. Para desarticular el DarkMarket, al FBI no le bastaría con arrestar a su líder, puesto que no existe. En su lugar, las fuerzas policiales se verían obligadas a ir tras los compradores y vendedores de artículos de contrabando uno por uno, algo prácticamente imposible que convierte la Red Oscura en unos verdaderos Campos Elíseos[*] para Crimen, S. A.

Para ayudar a los delincuentes y *hackers* neófitos a navegar por la Internet Profunda, los mercados ilícitos han establecido útiles *wikis* ocultas, una suerte de *Crimenopedia*s perfectamente organizadas por categoría y con enlaces a otros sitios

.onion. Entre esas categorías figuran ataques informáticos, manipulaciones de sistemas telefónicos, anarquía, *warez* o *software* ilegal, virus, mercados, drogas y erotismo, cada una con enlaces y descripciones de lo que puede encontrarse en ellas. Mas incluso con la ayuda de los wikis, navegar por la Red Oscura puede suponer todo un reto y encontrar la droga, el arma o el asesino exactos que se buscan puede ser tarea ardua. A tal fin, a mediados de 2014 un *hacker* sumamente innovador creó el primer motor de búsqueda distribuida de la Internet Profunda, conocido como Grams[16]. Cortado por el patrón de Google, únicamente es posible acceder a Grams a través del navegador de Tor que garantiza el anonimato y utilizando una dirección .onion. Con Grams, quienes buscan contrabando pueden introducir sus palabras clave y realizar búsquedas de bienes y servicios en ocho mercados negros distintos de manera simultánea. El motor de búsqueda devuelve el nombre de un vendedor y permite efectuar compras comparativas. Al igual que Google, incorpora un botón «Voy a tener suerte», que, al clicarse, puede conducir a los usuarios a un sitio de «*crystal meth* de alta calidad». En su función de prototipo a lo Google para el delito, Grams incluso acepta publicidad y varios cárteles pueden competir por clientes adquiriendo términos de búsqueda por palabras clave. Como lo oyes: la búsqueda de «heroína marrón afgana» en Grams devolverá todos los resultados disponibles en la Internet Profunda, pero aquellos miembros de Crimen, S. A. que paguen una cuota conseguirán que su nombre aparezca entre las primeras posiciones en los resultados de la búsqueda, exactamente lo mismo que sucede con los anuncios patrocinados en Google. El hecho de que Grams ofrezca un programa de AdWords a la clandestinidad digital demuestra tanto la ávida perspicacia empresarial técnica como la sofisticación de Crimen, S. A.

Pese a que las búsquedas con anuncios patrocinados han llegado a la clandestinidad digital, no a todos los comerciantes ilegales les seduce la idea de ser localizables por las masas de delincuentes y, por ende, también por los cuerpos de seguridad. De ahí que en los dominios más discriminatorios de la Internet Profunda, como en el mundo real, los delincuentes necesiten que alguien los presente y ponga las manos en el fuego por ellos antes de poder negociar. Aquí, «la distribución de los bienes y servicios se organiza en miles de chats ilegales y foros sólo por invitación». Para acceder a los dominios ilícitos más exclusivos, uno necesita ir pertrechado con una dirección alfanumérica secreta, que no esté catalogada ni listada en ningún otro sitio en Internet, sino que pase de mano en mano. Determinados foros de delincuentes, como el sitio de *carders* ruso Maza, un mercado en línea gigantesco de tarjetas de crédito robadas, vetan la entrada a los aspirantes a sus mundos clandestinos a menos que sean aprobados de manera unánime por los miembros sénior de la organización y únicamente tras un período de espera de ocho días[17]. Ahora bien, una vez te aceptan en la élite de los *digerati* delincuentes, el mundo es tu ostra.

Navegar por el cuerno de la abundancia de las mercancías tabúes e ilícitas

disponibles en la clandestinidad digital puede parecerse a un largo descenso por los nueve círculos del infierno de Dante, en el que cada paso te conduce a un abismo más aterrador y profundamente inquietante. Lo que sigue no es más que una muestra somera de los bienes y servicios disponibles en los recovecos más tenebrosos de Internet, listados desde los más banales hasta los más espeluznantes.

CONTENIDO PIRATEADO.

Existen numerosos sitios web ilegales de «torrents» o archivos compartidos entre pares, como Pirate Bay, que figura entre los cien sitios web más visitados de Internet[18]. Otro sitio de estas características, el neozelandés Megaupload.com, recibió en su momento álgido cincuenta millones de «clientes» al día y registraba un cuatro por ciento del tráfico global en Internet[19]. Las autoridades y cuerpos de seguridad internacional mantienen que el propietario del sitio web era un *hacker* de nacionalidad alemana y expatriado de dos metros de altura y 160 kilos de peso conocido por sobrenombre de Kim Dotcom. Según las autoridades, los principales productos de Megaupload eran cincuenta petabytes (cincuenta y dos millones de gigabytes) de películas, canciones, videojuegos, libros y *software* robados. En Megaupload, el viento soplaba a favor y se calcula que la empresa generaba unos veinticinco millones de dólares al año en publicidad online y ciento cincuenta millones adicionales en las cuotas que pagaban los usuarios que querían robar el contenido descargable más rápidamente. Estos beneficios permitían a Kim Dotcom disfrutar de un estilo de vida salvajemente opulento en su mansión de veinticuatro millones de dólares, con 240 hectáreas de prados bien podados, pistas de tenis y su campo de golf personal. Entre otras posesiones de Kim Dotcom destacan un helicóptero, un megayate, quince Mercedes, un Rolls-Royce Phantom Drophead Coupé (precio de venta sugerido por el fabricante a partir de 474 600 dólares) y una cama Hästens sueca de pelo de caballo fabricada a mano por un precio de 103 000 dólares. La piratería es, sin duda, un negocio rentable.

DROGAS.

Tal como hemos visto en el caso de Silk Road, en la clandestinidad digital pueden adquirirse drogas ilegales y medicamentos con receta médica de todo tipo en cantidades que van desde el uso personal hasta ventas al por mayor entre traficantes. Con todo, Silk Road no es en absoluto el único mercado de narcóticos de la Internet Profunda, sino que existen centenares de sitios web de este género. En ellos, no sólo se venden las drogas estándar, como marihuana, heroína, éxtasis y cocaína, sino que además ofrecen productos mucho menos frecuentes, como escopolamina, el polvo

conocido como «Aliento del Diablo» empleado como droga de zombificación ofensiva, el cual, cuando se sopla sobre el rostro de una víctima, la deja consciente pero sin voluntad propia[20]. Minutos después de ser absorbido, el polvo inodoro e insípido otorga a ladrones, cacos y violadores control absoluto sobre sus víctimas y, lo que es peor, borra por completo en ellas el recuerdo de los detalles del incidente.

DINERO FALSIFICADO.

En la clandestinidad digital existe dinero falsificado a espuertas y los costes de adquirirlo varían en función de la calidad de la falsificación, de la cantidad adquirida y del tipo de divisas, entre las cuales se incluyen dólares, euros, libras y yenes. Sitios ocultos por Tor como Guttemberg Print, Cheap Euros y WHMX Counterfeit ofrecen billetes de alta calidad a veinticuatro centavos por dólar (de modo que con 600 dólares reales pueden adquirirse 2500 dólares falsos[21]). Los vendedores prometen que todos los billetes pasarán los test de luz ultravioleta y bolígrafo destinados a detectar los billetes falsos.

PRODUCTOS ELECTRÓNICOS/ARTÍCULOS DE LUJO ROBADOS.

En sitios de la Internet Profunda como Tor Electronics, CardedStore y Buttery Bootlegging se ofrecen productos electrónicos y artículos de lujo nuevos de fábrica con un descuento especial para la Red Profunda. Sus anunciantes ofrecen «artículos caros de los principales comercios a una fracción de su precio». Por supuesto, estos artículos se han robado, se han desviado de la fábrica o se han caído misteriosamente de los camiones de reparto.

TARJETAS/CUENTAS.

Quizá el artículo más abundante en la clandestinidad digital sean las tarjetas de crédito robadas, ampliamente disponibles en los llamados foros de «tarjeteros», donde las personas pueden comprar y vender tarjetas de crédito y débito prácticamente de cualquier banco y país del mundo. Todos los datos financieros robados mediante *software* malicioso, pirateo informático y extractores de tarjetas de crédito acaban a la venta en la Internet Profunda mediante «descargas de datos». Las descargas de datos aluden a los datos codificados en la banda magnética de una tarjeta de crédito e incluyen detalles como el nombre del titular, el número de la tarjeta, la fecha de caducidad y el CVV (valor de verificación de la tarjeta). Una vez sustraída, los delincuentes utilizan esta información para efectuar compras en Internet

o incluso para codificar los datos en nuevas tarjetas de plástico fraudulentas, que luego utilizan para ir a comprar «mercancía a altos precios que puede revenderse fácilmente a cambio de efectivo»[22]. Dados los inmensos volúmenes de robo de tarjetas de crédito, los precios por tarjeta robada en la clandestinidad digital han ido a la baja (de unos tres dólares en 2010 a sólo uno en 2013[23]). Las descargas de datos de las tarjetas de crédito robadas dan prueba de la elasticidad del mercado y, tras una infiltración masiva, como la de la intrusión en los comercios Target en 2013, los precios de tarjetas robadas se desplomaron debido a que la oferta superaba a la demanda del mercado. Las tarjetas se venden en sitios de la Red Oscura como Mazafaka, Tortuga, CarderPlanet, ShadowCrew, Approven.su y, mi favorito, IAACA (International Association for the Advancement of Criminal Activity o Asociación Internacional para el Avance de la Actividad Criminal[24]). Casi todos estos sitios exigen estar registrado y los miembros suelen someterse a aprobación para mantener al margen a la policía. Los tarjeteros prometen «altas tasas de validez» y ofrecen garantías del 95 por ciento de que sus tarjetas de crédito robadas funcionarán o «¡te devolvemos tu dinero!». Los beneficios que obtienen los tarjeteros implicados en este negocio son impactantes, con más de once mil millones de dólares perdidos en fraudes de pagos con tarjeta en todo el mundo cada año. Estados Unidos es la víctima principal de estos robos, con el 47 por ciento de la actividad con tarjetas fraudulentas de todo el mundo[25].

USURPACIÓN DE IDENTIDAD.

El uso ilegítimo de información identificable personalmente (IIP) es una práctica corriente en la clandestinidad digital. La información se filtra a través de agentes intermediarios de datos no seguros, sitios de redes sociales y el manejo poco sólido de los datos médicos, financieros, educativos, fiscales y de las transacciones de compras virtuales. Los piratas informáticos suelen referirse a estas identidades usurpadas con el nombre de «fullz» e incluyen nombres, direcciones postales, números de la Seguridad Social, fechas de nacimiento, lugares de trabajo, números de cuenta bancaria, códigos de identificación bancaria, números de permiso de conducir, los dos apellidos, direcciones de correo electrónico y nombres de usuario y contraseñas en Internet adicionales. Cerca del 20 por ciento de los ciudadanos de Estados Unidos y la Unión Europea han sido víctimas de usurpación de identidad, y los beneficios generados por las ventas de IIP a través de la Internet Profunda son monumentales[26]. El robo de identidades médicas (falsas afirmaciones con documentos de identidad falsificados) cuesta al sistema de sanidad pública de Estados Unidos 5600 millones de dólares al año, mientras que el robo de identidad en el caso de la declaración de la renta (es decir, que alguien presente una declaración de la renta a devolver en tu nombre y se embolse la devolución) costará a la Hacienda

Pública de Estados Unidos, el IRS, 21 000 millones de dólares en los próximos cinco años… todo ello porque filtramos cantidades ingentes de datos a través de sistemas profundamente inseguros con los que se puede comerciar y obtener unos beneficios descomunales en la Red Oscura[27].

DOCUMENTACIÓN.

En Internet es posible adquirir cualquier documento, ya sean pasaportes, permisos de conducir, papeles de ciudadanía, documentos de identidad falsos, diplomas universitarios, transcripciones, documentos de inmigración e incluso tarjetas identificativas diplomáticas. Empresas en la Red Oscura como Onion Identity Services venden pasaportes y carnets de identidad a cambio de bitcoins. Estos documentos van a parar a manos de delincuentes y terroristas, a quienes facilitan su libre movimiento a través de las fronteras internacionales, hacerse con nuevas identidades y blanquear dinero. Los permisos de conducción de calidad máxima de cualquier estado de Estados Unidos suelen enviarse desde China o Rusia y cuestan en torno a 200 dólares, mientras que los pasaportes de Estados Unidos o el Reino Unido están valorados en unos cuantos miles de dólares[28].

ARMAS, MUNICIÓN Y EXPLOSIVOS.

En la Internet Profunda, en sitios como Armory, Black Market Reloaded y LiberaTor, puede conseguirse casi cualquier arma que se quiera. Revólveres como Glocks, Berettas y pistolas automáticas de 9 mm con silenciadores son un artículo común a la venta. También se encuentran rifles de asalto, incluidos AK-47 y Bushmaster M4 (utilizados por las Fuerzas Especiales en Afganistán y capaces de disparar entre 700 y 950 balas por minuto en el modo automático integral), sin necesidad de tiempos de espera ni comprobaciones de antecedentes[29]. También hay en *stock* explosivos C-4 de un proveedor que anuncia alegremente «envíos a todo el mundo». Por supuesto, los envíos sí que suponen un cierto problema: no se puede enviar por FedEx un Uzi sin que suenen las alarmas. Los proveedores de armas en la Red Oscura han superado este obstáculo y envían sus productos en un embalaje protegido y camuflado para hacerlos pasar por otros artículos. Las armas de fuego se desmontan en piezas pequeñas y se envían mediante transporte especial. Los comerciantes incluso son capaces de conseguir «zulos» en un parque, un vertedero o un callejón donde ocultan las armas de fuego completamente montadas. Tras efectuar el pago, los compradores reciben las coordenadas de GPS y las descripciones de dónde se encuentran escondidos los productos. Hoy en día incluso hay disponible en Internet armamento de nivel militar. Un usuario de la Internet Profunda conocido como Bohica ofrece

principalmente armas pequeñas, pero afirma: «Si necesitas artillería, MANPADS [sistemas de defensa aérea portados por hombre], APC [transporte blindado de personal] o Helos, tenemos recursos y podemos realizar las presentaciones por una comisión. Envíanos tu siguiente mensaje con encriptación PGP; encontrarás nuestra clave pública en la página de nuestro perfil»[30].

ASESINOS A SUELDO.

Como hemos visto en el caso de Silk Road, los asesinatos pueden contratarse con sólo un clic en la Red Oscura. Proveedores de servicios como Killer for Hire, Quick Kill, Contract Killer y C'thulhu anuncian «soluciones permanentes a problemas comunes». Los mercenarios que ofrecen estos servicios se vanaglorian de su formación militar en cuerpos del ejército como la French Foreign Legion o presumen de su destreza como francotiradores perfeccionada en Irak o Afganistán. Cada servicio tiene unas reglas y regulaciones propias. Uno de ellos aplica una «política estricta de no menores» y se niega a asesinar a menores de dieciocho años, mientras que otro pone reparos a los asesinatos políticos. Pero no pasa nada, también hay multitud de servicios consagrados a asesinar a funcionarios gubernamentales, como el Assassination Market mencionado con anterioridad, que funciona mediante proveimiento participativo[31]. Los precios varían de unos escasos 20 000 dólares a más de 100 000 por matar a un agente de policía. Los sitios solicitan que proporciones una fotografía reciente del objetivo, así como la dirección de su domicilio y su lugar de trabajo, sus rutinas diarias y los lugares de ocio que frecuenta[32]. Los pagos en bitcoins son bienvenidos y lo habitual es que se envíe una prueba fotográfica del crimen cometido.

IMÁGENES DE PEDOFILIA .

De manera inquietante, la Red Oscura es un santuario para comerciantes de pornografía infantil, que se ofrece ampliamente en sitios Tor clandestinos como Hard Candy, Jailbait, Lolita City, PedoEmpire y Love Zone. The Family Album ofrece «material sexual privado y exclusivo rodado por los miembros» y es un auténtico YouTube de pedofilia autoproducida y grabada en vídeo. Kindergarten Porn provee enlaces por edad y género de los menores[33]. También hay a la venta libros electrónicos con títulos como *Cómo producir porno infantil para tontos* y *Cómo hacer el amor con niños*. Muchos sitios permiten a los pedófilos conectarse y comunicarse entre sí con el fin de compartir fantasías o imágenes. Asimismo, se intercambian tácticas detalladas sobre cómo apuntar de manera efectiva a un objetivo, seducirlo y realizar actos sexuales con niños. El volumen de estas actividades es

abrumador. Un solo sitio de la Internet Profunda tenía más de veintisiete mil pedófilos registrados en sus foros[34]. Es más, el Centro Nacional de Niños Desaparecidos y Víctimas de Abusos Sexuales de Estados Unidos examina cerca de veinte millones de imágenes de pederastia al año, un incremento del 4000 por ciento desde 2007[35]. Fuentes de los cuerpos de seguridad informan de que el 19 por ciento de los pedófilos tienen imágenes de abusos sexuales cometidos con niños menores de tres años, el 39 por ciento de niños menores de seis años y el 83 por ciento de niños menores de doce años[36]. En toda la Internet Profunda, los pedófilos experimentados dan lecciones sobre cómo evadir a las autoridades policiales y debaten técnicas de encriptación y anonimato para evitar ser detectados en Internet.

TRÁFICO DE PERSONAS.

La Internet Profunda también facilita el tráfico de seres humanos y existen numerosos sitios web especializados en la compraventa de adultos y niños. El Departamento de Justicia de Estados Unidos calcula que el tráfico de personas genera más de 32 000 millones de dólares al año en efectivo a Crimen, S. A.[37] Mientras que los canales tradicionales de tráfico siguen operativos, las tecnologías en Internet brindan a los traficantes «la capacidad sin precedentes de explotar a un mayor número de víctimas y anunciar sus servicios sin fronteras geográficas». Sólo en Estados Unidos se trafica con unos 200 000 niños con fines sexuales y un proxeneta puede ganar entre 150 000 y 200 000 dólares al año por niño. Aproximadamente el 70 por ciento de los supervivientes del tráfico infantil afirman que se los anunció en Internet en algún momento mientras estaban en el mercado y se los forzaba a mantener relaciones sexuales hasta veinte veces al día[38]. Estas actividades no se negocian sólo a través de la Internet Profunda, sino también en redes sociales relativamente abiertas y en anuncios clasificados de la Red superficial[39]. Sitios web como BackPage.com prometen «acompañante» y «masajes» y los anuncios de proxenetas reportan cerca de cuarenta y cinco millones de dólares al año en ingresos a las empresas de anuncios clasificados online[40]. Sin embargo, en Internet no sólo se trafica con niños, sino también con inmigrantes y otras poblaciones en riesgo.

TRÁFICO DE ÓRGANOS HUMANOS.

Existe en todo el mundo un mercado negro de órganos humanos tan floreciente como atroz[41]. Los riñones alcanzan los 200 000 dólares; los corazones oscilan los 120 000; los hígados se venden por unos 150 000 dólares y la piel a sólo diez dólares por 2,5 cm^2; un hombro vale 500 dólares y un par de globos oculares, 1500 dólares[42]. ¿De dónde proceden estos pedacitos de humanidad? Tanto de seres vivos

como de muertos. El saqueo de tumbas sigue siendo una actividad ferviente en el siglo XXI, y muchas morgues de todo el mundo venden partes de los cadáveres confiados a su cuidado, asumiendo correctamente que la familia nunca se enterará. Lo que es peor, los seres humanos pobres y vivos corren un riesgo muy particular, pues se los convierte en objetivo tanto en Internet como en la vida real para que vendan sus órganos a pacientes ricos que los necesitan desesperadamente. Sólo en Estados Unidos hay más de 100 000 personas en lista para recibir riñones, lo cual representa una espera de diez años[43]. La mayoría de esas personas morirán en la mitad de ese tiempo[44]. De ahí que los pacientes adinerados se dirijan a ultramar en busca de «donantes» y conduzcan un floreciente tráfico ilícito de órganos humanos. Crimen, S. A. cuenta con toda una división de agentes dedicados a la compraventa de órganos, los cuales ejercen de intermediarios en distintos continentes para conectar a compradores y vendedores, a quienes proporcionan las indicaciones para que se dirijan a médicos, cirujanos e instalaciones médicas asociadas con ellos. La Organización Mundial de la Salud calcula que en estas redes clandestinas se obtiene ilegalmente un órgano cada hora[45]. Los órganos pueden proceder de presos ejecutados en China, de mujeres en la India a quienes sus maridos obligan a vender partes de su cuerpo para contribuir a la economía familiar o de refugiados sirios recién llegados al Líbano y desesperados por obtener dinero en efectivo[46]. Pese a que un riñón puede venderse por 200 000 dólares, quienes lo donan cobran mucho menos, entre 2500 y 10 000, lo cual genera un margen de beneficios nada desdeñable a los traficantes. Por desgracia, quienes venden sus órganos reciben pocos o nulos cuidados postoperatorios y muchos mueren tras la cirugía[47]. Cada vez más estas actividades tienen lugar en Internet, en chats y a través de la Internet Profunda. Los pobres de lugares como India, Bulgaria y Serbia publican solicitudes desesperadas, como la de una ama de casa que especificaba su tipo sanguíneo y su número de teléfono y había escrito: «Vendo mi riñón, mi hígado y haré lo que sea para sobrevivir»[48]. En China, los traficantes de órganos se dirigen especialmente a los jóvenes a través de foros de Internet con eslóganes como «Dona un riñón y cómprate el nuevo iPad»[49]. Se sabe que al menos un adolescente de diecisiete años, ahora con una salud frágil, aceptó el trato: su madre descubrió el nuevo iPad en el hogar familiar, de estrato pobre, y acudió a la policía[50].

VIOLACIÓN DE MENORES EN DIRECTO.

Como el *Inferno* de Dante, la Internet Profunda tiene sus propios nueve círculos infernales y aquí es donde hallarás los actos de violencia más abominables contra los miembros más jóvenes y vulnerables de nuestra sociedad. En un informe hondamente perturbador publicado por la Europol, el organismo policial de la Unión Europea, miembros de los cuerpos de seguridad destacaban el número creciente de sitios web

clandestinos que en la actualidad proporcionan vídeos en directo de abusos y violaciones de niños[51]. De hecho, Crimen, S. A. y las redes pedófilas están organizando violaciones a menores bajo demanda mediante la técnica de pago por visualización. En particular, redes de la delincuencia organizada en Asia proporcionan a los pedófilos la capacidad de conectarse en directo mediante Tor a canales de vídeo con funciones de mensajería instantánea incorporadas donde los usuarios de todo el mundo pueden solicitar a los violadores que han secuestrado a los menores que perpetren abusos específicos[52]. En efecto, por nauseabundo que suene, aceptan peticiones. En un incidente investigado por la policía, quienes se conectaban a través de Tor podían solicitar a un grupo de hombres que violaran a una niña de ocho años, dirigiendo sus acciones en tiempo real, y todo ello por cien dólares[53]. Puesto que estas actividades tienen lugar en la Internet Profunda y dado que las imágenes en vídeo se transmiten en tiempo real, en lugar de descargarse, las pruebas para demostrar estos delitos no quedan grabadas en ningún sitio, salvo en los recuerdos permanentes y traumáticos de las víctimas que sobreviven a la brutalidad depravada de otro ser humano.

Todos estos bienes y servicios ilícitos a la venta en la clandestinidad digital reportan pingües beneficios a Crimen, S. A., una tendencia que se está acelerando gracias a las nuevas formas de financiación ilícita que facilitan enormemente sus operaciones empresariales ilegales.

Monedas oscuras

Bictoin se ha expedido. Pero no compite con la perfección.

DAN KAMINSKY, investigador de temas de seguridad

La tecnología está haciendo posibles nuevas formas de dinero y la economía digital en expansión promete proporcionar nuevas herramientas financieras, sobre todo a los pobres del mundo y a aquéllos sin acceso a la banca. Estas divisas virtuales emergentes suelen ser anónimas y ninguna de ellas ha recibido tanta prensa como bitcoin, una forma digital de dinero entre pares descentralizada. Los bitcoins fueron inventados en 2009 por una misteriosa persona (o un grupo de personas) con el sobrenombre de Satoshi Nakamoto. Se trata de monedas creadas o «minadas» mediante la resolución de ecuaciones matemáticas de dificultad creciente, para la cual se requiere una gran capacidad computacional. El sistema está diseñado para garantizar que no puedan generarse nunca más de veintiún millones de bitcoins, gracias a lo cual se impide que una autoridad central pueda inundar el mercado con bitcoins nuevos[54]. La mayoría de las personas compran bitcoins mediante el cambio

de divisas tradicionales, como dólares o euros, con terceros, si bien también pueden adquirirse con tarjetas de crédito. El tipo de cambio del bitcoin frente al dólar fluctúa sobremanera y ha ido desde cincuenta céntimos por moneda en torno a la fecha de su lanzamiento hasta más de 1240 dólares por bitcoin en noviembre de 2013.

Las personas pueden enviarse bitcoins entre sí mediante ordenadores o aplicaciones móviles, donde las monedas se almacenan en «monederos digitales». Los bitcoins pueden intercambiarse directamente entre usuarios de cualquier parte del mundo utilizando identificadores alfanuméricos únicos similares a direcciones de correo electrónico y no se aplican comisiones por transacción. Cada vez que se efectúa una compra, se graba en un libro de contabilidad público conocido como la «cadena de bloques», que garantiza que no se autoricen transacciones duplicadas. Bitcoin es la criptomoneda más extendida del mundo, así llamada porque utiliza «criptografía para regular la creación y transferencia de dinero, en lugar de confiar en autoridades centrales»[55]. La aceptación de bitcoins se extiende cada vez más y ya es posible utilizar la moneda para comprar magdalenas en San Francisco, cócteles en Manhattan y un sándwich Subway en Allentown. También pueden emplearse para adquirir un nuevo Tesla Modelo S, pagar la factura de DIRECTV, registrarse en OkCupid o incluso para reservar una entrada para el futuro vuelo espacial con Virgin Galactic de Richard Branson.

Dado que los bitcoins pueden gastarse en Internet sin necesidad de disponer de cuenta bancaria y que no se requiere ningún documento identificativo para comprar y vender criptomonedas, proporciona un sistema práctico para realizar transacciones anónimas o, mejor dicho, con seudónimo, en las que el verdadero nombre del usuario queda oculto[56]. A pesar de que los bitcoins, como todas las formas de dinero, pueden usarse para fines tanto legítimos como ilegítimos, sus técnicas de encriptación y su anonimato relativo revisten un fuerte atractivo para los delincuentes. Y al no estar los fondos almacenados en ninguna localización central, no es posible congelar las cuentas ni investigarlas, y rastrear las transacciones grabadas en la cadena de bloques es considerablemente más complejo que presentar una citación a una sucursal bancaria local que opere en las redes financieras tradicionalmente reguladas. Como consecuencia, casi todo el comercio ilícito que tiene lugar en la Internet Profunda lo propician los sistemas de divisas alternativas. Nadie paga metanfetamina o imágenes de abusos sexuales a menores con un cheque en papel o una tarjeta de crédito. Los métodos preferidos de pago en estos casos son formas digitales y virtuales anónimas de dinero, como los bitcoins.

En los días de la mafia de Al Capone, durante la Prohibición, el mantra del FBI pasó a ser «Sigue el dinero» y finalmente fueron cargos de evasión fiscal, y no ninguna condena por asesinato, lo que acabó derribando al mayor capo del crimen organizado mundial de la década de 1930. Pese a que «Sigue el dinero» ha sido el credo nuclear de los cuerpos de seguridad desde entonces, es posible que la policía deba buscar uno nuevo en breve. Actualmente hay más de setenta criptomonedas

virtuales que compiten con Bitcoin, como Ripple, Litecoin y Dogecoin, y se calcula que sólo en 2013 se tramitaron cerca de diez mil millones de dólares en monedas virtuales[57]. Dadas las inmensas sumas en juego, no debería sorprender que los delincuentes no sólo utilicen bitcoins en sus operaciones sino que también dirijan sus ataques contra la criptomoneda. Los *hackers* han logrado robarse entre sí millones y millones de dólares en dinero virtual[58]. El robo más importante hasta la fecha se dirigió contra Mt. Gox, una casa de cambio de bitcoins con sede en Tokio, que vio cómo le birlaban 470 millones de dólares de sus cofres digitales a principios de 2014. Sin duda alguna éste es el futuro de los robos bancarios y, por si te asalta la duda, no, la Corporación Federal de Seguros de Depósitos estadounidense (FDIC) no cubre las pérdidas en bitcoins.

Además de las criptomonedas, hay muchas otras formas de pago electrónico favorecidas por Crimen, S. A., incluidas entre ellas Liberty Reserve, E-gold y WebMoney[59]. Sobre una sola de estas empresas, Liberty Reserve, pesan acusaciones de haber blanqueado más de seis mil millones de dólares en varios años, de acuerdo con la Fiscalía General de Estados Unidos. Conocida como «el PayPal de los delincuentes», donde no se precisan detalles de cuenta personales, Liberty Reserve propició una amplia gama de actividades de Crimen, S. A. en la Internet Profunda, incluidas entre ellas «fraude con tarjetas de crédito, usurpación de identidad, fraude de inversiones, pirateo informático, pornografía infantil y narcotráfico»[60]. También se cree que la empresa desempeñó un papel crucial en el asalto y robo de cuarenta y cinco millones de dólares a través de cajeros automáticos organizado mediante una operación de proveimiento participativo que hemos explicado antes, perpetrado durante un lapso de diez horas en 2013. Pese a que Liberty Reserve, como Silk Road, acabó por ser desarticulada por el FBI y su fundador fue arrestado, muchos competidores han ocupado su hueco y estos nuevos mercados suelen contar con estructuras entre pares descentralizadas y propician las iteraciones de criptomonedas de la próxima generación. No sólo prometen registrar públicamente las operaciones bajo seudónimo, como ocurre en la cadena de bloques de Bitcoin, sino un anonimato completamente imposible de rastrear. Una de estas monedas nuevas, Darkcoin, puede considerarse la prima ultrasecreta a la sombra de los bitcoins, creada específicamente para velar las compras de los usuarios mediante la combinación de cualquier transacción con las de otros usuarios, de manera que los pagos no puedan vincularse a una persona concreta. Darkcoin gana popularidad a un ritmo acelerado y su valor se ha disparado por los aires de los setenta y cinco centavos iniciales por una moneda a los casi siete dólares poco después de su introducción[61].

Otra herramienta, Darkwallet, creada por una organización que se autodefine como unSYSTEM, aboga por devolver los bitcoins a sus raíces libertarias permitiendo transacciones «hiperanónimas». Con el lema «Que se haga la oscuridad», Darkwallet «pretende ser la aplicación de bitcoins anarquista favorita» y sus creadores la describen sin tapujos como un «*software* para blanqueo de

dinero»[62]. Combinando y encriptando pagos de los usuarios, Darkwallet «posibilita flujos de dinero prácticamente imposibles de rastrear» por la clandestinidad digital. Armados con estas nuevas herramientas económicas, los delincuentes están listos para salir de compras… y hay mucho donde escoger.

El delito como servicio

Con un sistema monetario ilegal en funcionamiento, los delitos han dejado de ser algo que sólo se comete para convertirse en algo que puede comprarse. El Crimen como Servicio (CaaS por sus siglas en inglés, de *Crime as Service*) es el nuevo modelo de negocio y permite que otros se encarguen de perpetrar parte o la totalidad de un delito, mientras que el empresario ilegítimo que ha organizado e invertido en el plan se lleva los beneficios. De la misma manera que las grandes empresas utilizan cada vez más el *Software* como Servicio para realizar operaciones empresariales ajenas a sus competencias esenciales, los delincuentes también han optado por este método.

Uno de los servicios que suele adquirirse con mayor frecuencia es el de infraestructuras de TI, las tripas y las tuberías tecnológicas necesarias para regentar cualquier empresa moderna de éxito. Ahora bien, Crimen, S. A. tiene unas necesidades de infraestructuras tecnológicas especiales, sobre todo con respecto a un bien cada vez más escaso: la privacidad y el anonimato. Los delincuentes han irrumpido en manada en la Internet Profunda porque les brinda las mejores oportunidades de evadir tanto los modelos empresariales de vigilancia popularizados por Facebook y Google como las capacidades a nivel estatal desveladas por Edward Snowden. Puesto que tanto su sustento como sus vidas dependen de permanecer en el anonimato, los integrantes de Crimen, S. A. dedican importantes recursos a preservar su privacidad antes de atacar a sus objetivos o vender sus artículos de contrabando.

En la práctica, esto significa que los agentes ilícitos que operan en la clandestinidad digital hacen un amplio uso de redes privadas virtuales (VPN) y servidores *proxy* para ocultar sus direcciones de protocolo de Internet y su localización. También dependen en gran medida de los llamados servicios de alojamiento a prueba de balas, empresas que proporcionan alojamiento web en jurisdicciones como Rusia y Ucrania y no ponen objeción a colgar contenido ilegal, no tienen interés en conocer las verdaderas identidades de sus clientes, aceptan pagos anónimos en Liberty Reserve y bitcoins y desoyen de manera rutinaria las citaciones de los cuerpos de seguridad. Una de dichas empresas de CaaS, Freedom Hosting, fue el servidor web más importante de la red Tor y fue acusado por el FBI de ser el facilitador más prolífico de imágenes de abusos sexuales a niños de todo el mundo, con más del 95 por ciento de la pornografía infantil alojada en sus dominios[63].

Centenares de empresarios ilegales proveedores de imágenes de abusos sexuales a niños pagaban a Freedom Hosting para que albergara de manera anónima sus sitios web clandestinos, cada uno de ellos con miles de suscriptores[64].

Además, de la misma manera que las empresas están adoptando rápidamente la computación en la nube para almacenar sus archivos en servicios como Google Drive o Amazon, Crimen, S. A. también opera en la misma línea. En un interesante vuelco de los acontecimientos, los piratas informáticos ya no sólo atacan los datos que almacenamos en la nube, sino que cada vez aprovechan más la facilidad de uso de este servicio para almacenar sus archivos menos comprometedores online. La nube es especialmente idónea para satisfacer las necesidades informáticas de los miembros de Crimen, S. A. que utilizan tarjetas de crédito robadas, identidades falsas y empresas fachada para alquilar espacio con empresas legales con el fin de albergar *software* dañino en sus servidores. Al utilizar el nombre de empresas con buena reputación para albergar su *crimeware*, es mucho menos probable que terceras partes detecten o bloqueen el tráfico de los *hackers*. Esta tendencia se está acelerando y un estudio realizado en 2013 sugería que el 16 por ciento de los canales de distribución de *malware* mundiales estaban albergados en Amazon Cloud, mientras que otro 14 por ciento emanaba de los servidores de GoDaddy[65].

Es más, la nube pone un tremendo poder computacional a disposición de usuarios legítimos y piratas informáticos por igual. Por ende, nos hemos adentrado en la era de la computación armada, donde, literalmente, cualquiera con unos cuantos dólares para invertir puede tener acceso a niveles de potencia informática previamente inimaginables, y usarlos para bien o para mal. Por ejemplo, los *hackers* que se colaron en la red de Sony PlayStation utilizaron el inmenso poder de computación de los servicios informáticos en la nube de Amazon para desbloquear varias claves de encriptación de Sony, lo cual les proporcionó acceso a cientos de miles de cuentas de usuario y detalles de tarjetas de crédito[66]. Este «agrietamiento de la nube» reduce significativamente el tiempo que se tarda en descifrar incluso las contraseñas más robustas y, en el proceso, hace que todos estemos menos seguros. Hoy en día, empleando el poder computacional distribuido de la nube y herramientas como CloudCracker, puedes probar trescientos millones de variaciones de tu contraseña potencial en unos veinte minutos por un coste de unos 17 dólares[67]. Ello implica que cualquiera podría alquilar servicios de computación en la nube de Amazon para descifrar la clave de encriptación normal que protege la mayoría de las redes Wi-Fi en menos de seis minutos, todo ello por la irrisoria suma de 1,68 dólares en tiempo de alquiler (cifra que seguramente bajará en el futuro gracias a la ley de Moore[68]).

Del mismo modo que las empresas legales contratan a programadores informáticos para armar sus sitios web y programar *software*, también lo hace Crimen, S. A. Una empresa como CrimeEnforcers (un juego de palabras con *law enforcers*, «cuerpos de seguridad») se describe como una «organización privada para tus solicitudes de desarrollo especiales […] Si necesitas *hardware* especial […] o

software que no pueda realizarse o incluso debatirse [*sic*] en tu país […], te ofrecemos programación completamente anónima y en el extranjero para tus proyectos. Nos da igual lo que pretendas hacer con el *hardware* y el *software* que nos solicites»[69]. Es decir, que en el mundo del desarrollo de *software* con fines delictivos no se formulan preguntas. También es posible contratar a empresas de Crimen, S. A. para infiltrarse en el sistema que se elija, empresas con potentes capacidades para hacerlo. A título de ejemplo, la organización china Hidden Lynx está integrada por hasta cien ciberladrones profesionales de quien se sabe que han penetrado en sistemas pertenecientes a Google, Adobe y Lockheed Martin, entre otros[70]. Lo que más asusta, no obstante, es que entre los miembros de Hidden Lynx hay militares y agentes de espionaje que trabajan para el gobierno chino durante el día y perpetran sus ciberoperaciones ofensivas en nombre del Estado. Cuando están fuera de servicio, muchos de estos funcionarios suplementan considerablemente sus ingresos pluriempleándose como estafadores virtuales y piratas informáticos de alquiler, sobresalientes en su campo por sus habilidades, muy superiores a las del *hacker* medio[71]. Bienvenido al mundo de los cibermercenarios, ahora disponible como una de las muchas ofertas de CaaS en la clandestinidad digital.

Además de los servicios de piratas informáticos de alquiler, Crimen, S. A. subcontrata una amplia variedad de servicios administrativos, como banca, traducción, viajes y operaciones en centros de atención telefónica.

Así por ejemplo, empresas como CallService.biz llenan un nicho en la clandestinidad digital proporcionando intérpretes de inglés, francés y alemán a demanda para ayudar a los ladrones a contravenir las medidas de seguridad bancarias necesarias para iniciar transferencias online, desbloquear cuentas pirateadas o intercambiar datos de los contactos de la agenda con los bancos. Con personal las veinticuatro horas, los siete días de la semana, el centro de atención telefónica plurilingüe para delincuentes representa cualquier papel falso que se le encargue, inclusive aportar referencias para empleos e instituciones educativas, por sólo diez dólares la llamada[72]. Cualquier servicio profesional que el empresario delincuente necesite puede contratarse en la clandestinidad digital. No obstante, cada vez son más los servicios de este tipo que se reúnen, organizan en paquetes y venden bajo la forma de *software* delictivo, ampliamente disponible en las profundidades de la Internet Profunda.

Crimenazon.com

La economía de la clandestinidad digital es compleja. No sólo los delincuentes venden directamente a los consumidores (drogas, falsificaciones de permisos de

conducción, contenido pirateado, etc.), sino que también se realizan ventas al por mayor entre sí. Si bien en gran medida, el Crimen como Servicio consiste en mantener la infraestructura de soporte y el anonimato requeridos para que la fábrica de los delitos siga echando humo, la economía sumergida se ha apuntalado a medida que los integrantes de Crimen, S. A. han empezado a ofrecer herramientas en paquetes preparados para *phishing*, correo no deseado, fraude, DDoS y robo de datos.

Los programadores delincuentes de primera se han dado cuenta de que las herramientas de pirateo ofensivo de las cuales se han dotado pueden reportarles beneficios si las venden a sus correligionarios (faltos de tiempo o de experiencia) con el fin de que éstos puedan perpetrar sus propios ataques. En consecuencia, delincuentes menos avezados pueden limitarse a adquirir las herramientas que necesitan a demanda para identificar vulnerabilidades de sistemas, cometer usurpación de identidad, infiltrarse en servidores y robar datos: delitos al alcance de un clic del ratón[73].

Así pues, la Internet Profunda se ha convertido en una «Crimenazon.com» virtual, el mercado en línea más extenso al cual pueden acudir los delincuentes. Allí hallarán un bazar turco de frutos prohibidos, todos ellos perfectamente dispuestos para su compra. Como otros proveedores de comercio electrónico, Crimen, S. A. ha creado la Red Oscura, escaparates de productos con sus carritos de la compra en línea, sistemas de gestión de pagos y finalización de pedidos, códigos de descuento, procesamiento de pagos, asistencia técnica, chats de atención al cliente en directo y servicios de fideicomiso. Los vendedores ofrecen servicios integrales y puedes dejar la American *Express* en casa, porque aceptan alegremente bitcoins[74].

A título de ejemplo, el *software* malicioso responsable de la invasión masiva del sistema de puntos de venta de Target a finales de 2013 se perpetró con un kit de herramientas de *crimeware* conocido como BlackPOS[75]. Entre algunos de los kits de herramientas delictivos más populares a la venta en la clandestinidad digital figuran los siguientes:

Zeus Builder: Con un precio de entre 5000 y 7000 dólares, el programa incorpora muchas funciones que van desde capturar de manera subrepticia pulsaciones de teclas de los usuarios hasta robar los certificados de encriptación digitales requeridos por la banca online. A lo largo de los años, Microsoft ha calculado que el troyano Zeus ha infectado más de trece millones de ordenadores en todo el mundo y se ha utilizado para robar más de cien millones de dólares[76].

Bugat: Con un precio de tan sólo 1000 dólares, Bugat se especializa en usurpar cuentas bancarias y simular solicitudes de transferencias bancarias. En 2010, Bugat se utilizó en un mensaje de correo electrónico de *phishing* que se envió a decenas de millones de usuarios de LinkedIn camuflado bajo un mensaje que decía «actualiza tu cuenta». Cuando así lo hacían, el troyano Bugat instalaba *malware* en sus navegadores web en menos de cuatro segundos y permanecía latente a la espera de robar sus datos financieros la siguiente vez que se conectaran a sus cuentas bancarias[77].

SpyEye: Por sólo 500 dólares, SpyEye ofrecía todas las funciones de Zeus y algunas más. Su lanzamiento al mercado a finales de 2009 desencadenó una guerra de precios de *crimeware* y su cuota de mercado se multiplicó rápidamente. En un vuelco fascinante de esta guerra entre bandas en Internet, los inventores de SpyEye incluyeron un módulo antivirus para detectar la presencia del troyano Zeus de su rival en las máquinas infectadas de usuarios del público general. Una vez lo

detectaba, SpyEye eliminaba alegremente la amenaza Zeus de la competencia y reparaba el punto de entrada para asegurarse de que SpyEye fuera el único *malware* que operaba en la máquina vulnerada[78]. Como su rival Zeus, se cree que SpyEye ha generado cientos de millones de dólares en beneficios a sus arquitectos[79].

Los kits de herramientas de *software* vendidos en Crimenazon.com se desarrollan sin cese, y Crimen, S. A. vende actualizaciones a sus «últimas versiones» para asegurarse de que sus programas incluyan las vulnerabilidades informáticas más recientes. Por supuesto, también hay un Crimenazon Prime, un programa que ofrece a otros mafiosos la oportunidad de «suscribirse y ahorrar» en sus compras. Un ejemplo de este tipo es el kit de herramientas Blackshades disponible a modo de alquiler continuo, que proporciona a los usuarios asistencia técnica y actualizaciones gratuitas ilimitadas. La herramienta, quizá uno de los kits de *exploits* de *software* malicioso más populares e infames, combina una agilidad técnica destacable con un modelo de negocios muy evolucionado que podría haber salido perfectamente de un caso de estudio de la Harvard Business School[80].

Los empresarios delincuentes que adquirían el kit de herramientas Blackshades podían seleccionar el modo como el *software* malicioso atacaría a una máquina concreta, por ejemplo: incrustando el troyano en un documento, ocultándolo en un sitio web o colocándolo en una unidad de USB que entregaría su carga envenenada cuando se insertara de manera inocente en el ordenador de destino. Puesto que Blackshades era un troyano de acceso remoto (RAT) avanzado, brindaba a sus artífices un control total y absoluto de las funciones de la máquina infectada. Por tanto, Blackshades podía capturar las pulsaciones del teclas, robar contraseñas, lanzar ataques de denegación de servicio, secuestrar cuentas de Facebook e instalar *malware* adicional en el sistema afectado. Peor aún, era la herramienta elegida por los acosadores, porque permitía a quienes la dominaban activar de manera remota el micrófono y la cámara de cualquier ordenador para captar audio y vídeo en su campo de visión, sin que se activara pista delatora alguna, como la lucecilla verde de grabación[81]. De hecho, el RAT Blackshades era tan eficaz que el régimen sirio de Bashar al-Assad lo utilizó para espiar a activistas defensores de la democracia en su país[82]. Pese a que es posible comprar multitud de kits de herramientas para delitos y espionaje «de apuntar y hacer clic» en Crimenazon.com, cada ataque de cada ordenador empieza con la infiltración en el sistema y la infección inicial con *malware*, vulnerabilidades que pueden conseguirse sin problemas en la clandestinidad digital.

El complejo industrial del *software* malicioso

> Los científicos nucleares perdieron la inocencia cuando utilizaron la bomba atómica por vez primera. Y podríamos decir que los científicos informáticos perdieron su inocencia en 2009, cuando empezamos a utilizar *software* malicioso como herramienta de ataque ofensiva.
>
> MIKKO HYPPONEN

Para que delincuentes, espías, militares y terroristas puedan perpetrar ciberataques ofensivos, primero deben averiguar cómo vulnerar el sistema de información que se han marcado como meta. Tal como hemos visto con relación al ataque de Stuxnet contra la planta de enriquecimiento nuclear iraní en Natanz, tales operaciones pueden llevar años de planificación y costar millones de dólares. Por suerte para aquéllos sin tiempo ni presupuesto para diseñar sus propias ciberarmas, existe un amplísimo mercado negro a la sombra donde espías, soldados, ladrones y *hacktivistas* pueden adquirir los llamados ataques de día cero. Como se ha explicado con anterioridad, estas vulnerabilidades no han sido descubiertas por los fabricantes de *software* y antivirus, lo cual permite superar cómodamente las medidas de seguridad y los cortafuegos habituales sin hacer sonar las alarmas.

En los viejos tiempos, los piratas informáticos solían aprovechar estos errores para uso personal e intentaban venderlos a gigantes de la informática como Microsoft, Yahoo! y Google a través de programas «bug bounty» o de detección de agujeros de seguridad. No obstante, las recompensas eran irrisorias: apenas quinientos dólares por descubrir importantes agujeros en la seguridad[83]. Frustrados, los *hackers* cayeron en la cuenta de que tenían opciones mucho más prometedoras a su alcance, incluidas entre ellas vender sus vulnerabilidades de seguridad en el mercado abierto a delincuentes y gobiernos. Esta constatación ha conducido al establecimiento de una red sumamente compleja de compradores, vendedores e intermediarios de agujeros de seguridad en lo que ha dado en conocerse como el complejo de la industria del *software* malicioso.

Antes de poder vender sus kits de herramientas para ciberdelincuentes perfectamente empaquetados, como SpyEye y Zeus, Crimen, S. A. debe recopilar una serie de vulnerabilidades para *software* malicioso y empaquetarlas en un *crimeware* para su uso por parte del público malhechor. Y lo hace financiando compras compulsivas de *exploits*, porque dispone del presupuesto para hacerlo. Se dice que un *hacker* conocido como Paunch contrató a un intermediario de agujeros de seguridad de terceras partes y le asignó un presupuesto de cien mil dólares para que recopilara las vulnerabilidades que luego él utilizaría en su kit de *exploits* dañino Blackhole. Para no ser menos, otro *hacker*, conocido por el alias de J. P. Morgan, publicó un mensaje en el foro de delitos Darkcode anunciando que contaba con un presupuesto de cuatrocientos cincuenta mil dólares para invertir en agujeros de día cero y utilizarlos en su kit de herramientas de *crimeware* de propiedad[84]. Los chats en la Red Oscura están repletos de solicitudes de compra de *malware* y abundan

publicaciones del estilo de: «¿Tenéis algún *exploit* de ejecución de códigos para Windows 7? […] En caso afirmativo, el dinero no es problema»[85].

Ahora bien, el comercio con ciberarmas no está restringido a los delincuentes; los servicios de seguridad gubernamentales también son compradores frecuentes de estas herramientas y utilizan a intermediarios externos para obtener su armamento técnico. Uno de estos intermediarios, conocido como Grugq, se ha consagrado como uno de los agentes de *exploits* favoritos, capaz de cerrar tratos importantes entre quienes descubren fallos en la seguridad y quienes buscan adquirirlos para aprovecharlos con fines operativos. En 2012, Grugq vendió una vulnerabilidad del sistema operativo para teléfonos móviles iOS a un contratista del gobierno de Estados Unidos por nada menos que doscientos cincuenta mil dólares (de los cuales él se llevó el 15 por ciento, su comisión habitual[86]).

Han surgido varias empresas profesionales cuyo negocio exclusivo es traficar con vulnerabilidades para *malware* informático con gobiernos. Empresas como Vupen en Francia, Netragard en Massachusetts, Endgame en Georgia, Exodus Intelligence en Texas y ReVuln en Malta venden activamente *exploits* ofensivos a clientes de todo el mundo[87]. Si bien algunas empresas de tráfico de vulnerabilidades de día cero seleccionan a sus clientes, otras venden a quien sea, desde Crimen, S. A. hasta infames dictadores, sin formular preguntas. El resultado, tal como señaló el célebre investigador en materia de seguridad Tom Kellermann, es que ahora cualquiera puede descargarse un *ciberkalashnikov* o una cibergranada de multitud de sitios web[88].

Muchas vulnerabilidades de día cero permiten realizar ataques furtivos y sofisticados contra objetivos específicos, lo cual da lugar a lo que los investigadores en temas de seguridad han denominado la «amenaza persistente avanzada» (APT por sus siglas en inglés, de *Advanced Persistent Threat*). Las APT combinan una exhaustiva investigación de los objetivos con un elevado grado de encubrimiento para mantener el dominio y control de un sistema marcado durante meses o años, y su uso está proliferando. Ocultarse, observar y esperar es el *modus operandi* de estos ciberataques y los buenos *hackers* siempre borran los registros del sistema para que no pueda saberse que han estado ahí. Tanto si lo ha desarrollado el gobierno de Estados Unidos, China o Crimen, S. A., la probabilidad de que un producto antivirus para consumidores medios detecte una de estas amenazas avanzadas persistentes es nula.

Stuxnet tal vez sea la APT más infame, pero está emparentada con Flame y Duqu, junto con muchas otras amenazas todavía por descubrir. Peor aún, ahora que Stuxnet, una herramienta desarrollada para atacar los sistemas de control industrial y desconectar los tendidos eléctricos, se ha puesto en circulación y está disponible para su descarga, Crimen, S. A. la ha estudiado en detalle y ya emula sus técnicas y código informático para urdir ataques muchísimo más sofisticados[89]. El profundo desafío que afronta la sociedad a raíz del surgimiento del complejo industrial del *software* malicioso estriba en que, una vez se utilizan estas armas ofensivas, tienen tendencia a

filtrarse al espacio abierto. Como resultado se ha dado una proliferación de ciberarmas de código abierto ahora ampliamente disponibles en la clandestinidad digital para que cualquiera las rediseñe y monte como crea conveniente. ¿Cuánto tardaremos en ver a alguien asir uno de estos cócteles Molotov digitales y arrojárnoslo con la intención de atacar nuestros sistemas de infraestructuras esenciales? Por triste que suene, ya se están preparando ataques de esta índole.

La red de los muertos vivientes: ataques de redes por robots zombis

Un apocalipsis zombi no es la situación más jovial.

DANAI GURIRA (*MICHONNE*)
en *The walking dead*

Una de las herramientas más potentes del arsenal de un *hacker* es una *botnet*, una red de robots integrada por ordenadores infectados que quedan sometidos al pirata informático. Las llamadas máquinas zombis, la máquinas infectadas, son esclavizadas para formar *botnets*, que pueden utilizarse para diversos delitos, como difundir *software* malicioso, perpetrar ataques DDoS, distribuir *spam* o albergar contenido ilícito. Tanto ordenadores como teléfonos móviles pueden ser reclutados para formar un ejército de *botnets* mediante una infección con *malware*, sobre todo el que instalan kits de herramientas de *crimeware* prefabricadas como Blackshades y SpyEye, ampliamente disponibles y a la venta en la clandestinidad digital.

Por desgracia, la carga dañina para las víctimas de estos kits de herramientas es doble: no sólo les robarán los datos de sus tarjetas de crédito, las credenciales de acceso a la banca y su identidad, sino que además dejarán a su paso una puerta trasera persistente en su sistema que proporcionará a Crimen, S. A. acceso perpetuo a su máquina para hacer lo que le plazca.

Mientras estás sentado escribiendo un documento de Word o leyendo un artículo de la CNN online, el dueño del *botnet* puede estar utilizando tu máquina de manera simultánea y subrepticia para realizar distintos servicios delictivos. ¿Alguna vez te has preguntado por qué el ordenador te va tan lento? Es posible que, sin saberlo, estés participando en un ciberataque continuo contra terceros, sin tener ni idea de lo que está sucediendo. Gracias por *tus* servicios.

Los *hackers* han externalizado y descargado su ataque en ti y tu ordenador, embrollándote de manera involuntaria en una conspiración delictiva internacional con ellos. Crimen, S. A. incluso puede reclutar tu ordenador y colocarlo en una red de pornografía infantil entre pares, y ocultar imágenes de abusos sexuales en tu disco

duro[90]. Al fin y al cabo, ¿por qué iba a arriesgarse a guardarlas en sus redes? Así que, a causa de la inseguridad de tu red y de tu incapacidad para proteger tus dispositivos digitales, ahora también estás participando en la economía de la ciberdelincuencia. Tal como Facebook te está monetizando y está extrayendo provecho de tu vida en Internet, también lo está haciendo Crimen, S. A.

Algunos de los *botnets* con peor reputación son Mariposa, Conficker y Koobface, si bien nuevas incorporaciones como Gameover Zeus están acaparando rápidamente su cuota de mercado. De acuerdo con el FBI, Gameover Zeus sólo controlaba más de un millón de ordenadores en todo el mundo y ocasionaba cien millones en pérdidas financieras[91]. A mediados de 2014, el *botnet* de mayores dimensiones conocido se llamaba ZeroAccess y en un día determinado tuvo bajo su control absoluto cerca de dos millones de ordenadores zombis[92]. A medida que los *botnets* se amplían, aumenta su poder ofensivo, pues estos dos millones de ordenadores pueden prepararse para perpetrar un ataque de negación de servicio distribuido contra cualquier objetivo seleccionado. Las ofensivas de DDoS consisten en inundar un sistema informático o sitio web con decenas de miles de peticiones de información falsas y conseguir que el sitio web quede bloqueado, fuera de línea y no permita enviar correos electrónicos, presentar páginas web, procesar pedidos ni realizar transacciones bancarias.

Como todas las herramientas y servicios de Crimen, S. A., es posible adquirir o alquilar *botnets* zombis en Internet, lo cual abarata el alcance de esta capacidad ofensiva para el público general. En la clandestinidad digital rusa, pueden adquirirse potentes *botnets* de DDoS por setecientos dólares o por sólo dos dólares a la hora, y una hora basta para derribar un centro de atención telefónica o sitio web típico[93]. De media se lanzan casi trescientos ataques de este tipo en todo el mundo cada día. Es más, la sofisticación de la amenaza va en aumento debido a que tanto Crimen, S. A. como agentes estatales como Irán y China aprovechan cada vez más el poder de la computación distribuida masiva de la nube para lanzar ataques DDoS[94]. Una red zombi, conocida como Storm.bot 2.0, a la venta en la clandestinidad digital a mediados de 2014 por sólo 3000 dólares, ha usurpado quince servidores en la nube mundiales y es capaz de generar unos inconmensurables trescientos gigabytes por segundo de tráfico de ataque, cantidad que, según se anuncia, es más que suficiente para «dejar sin conexión a Internet a países pequeños». El resultado de estos robots informáticos zombis ha sido que Crimen, S. A. ha iniciado una carrera armamentística en el ciberespacio.

La cuota de víctimas afectadas por este tipo de extorsión virtual mediante *botnets* está aumentando e incluso empresas de perfil alto como Evernote y MeetUp.com han sufrido ya ataques[95]. La colección de kits de herramientas de *malware* y los millones de robots informáticos zombis que hay diseminados por todo el mundo están proporcionando a Crimen, S. A. potentes medios de dominio que pueden emplearse como armas ofensivas, máquinas para generar dinero o ambas cosas. Así pues, nos

hemos adentrado en la Era Industrial del Delito, con programación informática maliciosa produciéndose como churros al estilo de las cadenas de montaje, específicamente desarrollada y programada para ejecutarse con el piloto automático, trabajando con denuedo día y noche en la comisión de delitos a la par que los *hackers* engrosan sus arcas mientras duermen.

Comisión de delitos «automágicamente»

Pese a que Crimen, S. A. busca mejorar de continuo su proceso empresarial, no siempre comete delitos nuevos. En la era de la ley de Moore, estas tareas se han automatizado casi por entero y pueden ejecutarse en un segundo plano a gran escala sin necesidad de una intervención humana significativa. La automatización de los delitos permite a las mafias transnacionales disfrutar de las mismas eficiencias y ahorro en costes que las empresas multinacionales obtuvieron al incorporar la tecnología para realizar sus funciones empresariales nucleares. Por eso hoy en día los *hackers* pueden robar a cien millones o más personas de manera simultánea, en lugar de hacerlo una por una, tal como vimos con el ciberataque contra Sony PlayStation y Target.

Los kits de herramientas para *exploits* como Blackhole y SpyEye cometen delitos «automágicamente», minimizando la necesidad de mano de obra humana y, por ende, reduciendo de manera espectacular los costes para Crimen, S. A. También permiten a los *hackers* seguir la «larga cola» de oportunidades y cometer millones de robos en pequeñas cantidades de manera que las víctimas no los denuncien y los cuerpos de seguridad no tengan modo de rastrearlos. Mientras que los objetivos concretos de alto valor (empresas, países, personas famosas, individuos con un alto valor neto u objetos de afecto o desprecio) se someten a ataques específicos e individuales, al público general suele atacárselo mediante *software* malicioso automatizado que actúa como una gran red de pesca digital que atrapa todo lo que encuentra en Internet con una vulnerabilidad que pueda aprovecharse. Dadas estas ventajas evidentes, en fecha de 2011 se calculaba que el 61 por ciento de todos los ataques en línea se lanzaban mediante kits de herramientas delictivas completamente automatizados, los cuales generaban unos beneficios sensacionales para los gobernantes supremos de la Internet Profunda que los orquestaban de manera experta[96]. Los delitos modernos han quedado reducidos y destilados a un programa de *software* que cualquiera puede ejecutar para obtener unos beneficios tremendos.

No sólo es posible utilizar las *botnets* y otras herramientas reiteradamente para atacar o lanzar ofensivas, sino que incluso permiten cometer delitos mucho más sofisticados, como extorsión, soborno y chantaje. En una versión actualizada de la estafa de las soluciones de «detección de virus» de la ucraniana Innovative

Marketing, con las que obtuvieron quinientos millones de dólares, Crimen, S. A. ha lanzado al mercado un nuevo torrente de *malware* que puede hacer rehén a tu ordenador hasta que abonas un rescate para poder volver a acceder a tus archivos. Conocido como *ransomware*, estas herramientas de ataque se incluyen en diversos kits de la Red Oscura, como Gameover Zeus. La estafa tiene múltiples variantes, incluida una que asegura proceder de los cuerpos de seguridad. En todo el mundo, los usuarios cuyos ordenadores se infectan con el troyano Reveton Trojan ven cómo sus máquinas se bloquean y en su pantalla aparece una nota, supuestamente procedente del FBI. El mensaje, con aspecto oficial y el logotipo a todo color del FBI, asegura que el ordenador del usuario se ha bloqueado por motivos como la «infracción de las leyes de propiedad intelectual federales contra el material descargado de manera ilegal» o porque «has estado viendo o distribuyendo contenido pornográfico prohibido».

Se informa a los usuarios que, para desbloquear sus ordenadores, deben pagar una multa que va de los doscientos a los cuatrocientos dólares y cuyo pago únicamente puede realizarse mediante un vale prepagado de Green Dot's MoneyPak, que, según se instruye a las víctimas, pueden adquirir en su supermercado Walmart o CVS local[97]. Para intimidar aún más a las víctimas y confirmar que se trata de un asunto político serio, Crimen, S. A. muestra de manera destacada la dirección IP del supuesto infractor en la pantalla, así como fragmentos de metraje de vídeo previamente capturado con la *webcam* de la víctima. La estafa ya se ha cobrado decenas de miles de víctimas en todo el mundo, con ataques localizados por país, idioma y organismo policial. De este modo, los usuarios del Reino Unido reciben una notificación de Scotland Yard, a los europeos les aparece un aviso de la Europol y las víctimas de los Emiratos Árabes Unidos ven la amenaza, traducida al árabe, y supuestamente procedente de la comisaría central de la policía en Abu Dhabi[98].

Ha surgido asimismo otro tipo aún más pernicioso de extorsión conocido como CryptoLocker, un troyano que realmente encripta todos los archivos del ordenador de la víctima, de manera que no pueda volver a leerlos o acceder a ellos[99]. Para mayor alarma, el *malware* presenta un reloj con cuenta atrás, a modo de bomba de relojería, que advierte a los usuarios de que sólo tienen cuarenta y ocho horas para pagar trescientos dólares o sus archivos serán destruidos de manera permanente. Similar a la amenaza «si quieres volver a ver a tus archivos con vida», estos programas de *ransomware* aceptan de buen grado pagos en bitcoins. El mensaje enviado a las víctimas no era una amenaza a la ligera. Mientras que el *ransomware* previo podía engañar a los usuarios ocultando temporalmente sus archivos, CryptoLocker utiliza una potente criptografía Advanced Encryption Standard de 256 bits para bloquear los archivos, de manera que resulten irrecuperables. Cerca de 250 000 personas y empresas alrededor del mundo han sufrido a manos de CryptoLocker, lo cual ha generado unos ingresos calculados en treinta millones de dólares para su creador[100].

Las herramientas de *ransomware* automatizadas han emigrado también a los

teléfonos móviles, donde han afectado a usuarios de dispositivos Android en varios países[101]. Ahora bien, el azote de CryptoLocker no sólo ha recaído sobre personas particulares, sino también sobre empresas, ONG e incluso organismos gubernamentales. De hecho, la infección más tristemente famosa de este virus fue la del Departamento de Policía de Swansea, en Massachusetts, que fue infectado cuando un empleado abrió un archivo adjunto a un correo electrónico. Para no perder sus expedientes policiales irremplazables en manos de CryptoLocker, la policía se vio obligada a abrir una cuenta en bitcoins y pagar un rescate de setecientos cincuenta dólares para recuperar sus archivos. El teniente de policía Gregory Ryan explicó a la prensa que no tenía ni idea de qué era un bitcoin ni de cómo funcionaba el *software* malicioso hasta que su departamento fue víctima de aquel ataque[102].

Como hemos visto a lo largo de todo este capítulo, adentrarse en este mundo puede llevarnos a un abismo siniestro y temible. En su seno, Crimen, S. A. ha concebido métodos operativos ultrasofisticados para vender cualquier cosa, desde metanfetaminas hasta abusos sexuales a niños reproducidos en tiempo real en línea. Crimen, S. A. ha adoptado rápidamente las herramientas de anonimato como Tor para establecer centros comerciales en la Red Oscura, y los servicios de asesoría para delincuentes como el pirateo informático y el asesinato a sueldo están al alcance de un clic con el ratón. Monedas digitales anónimas y no rastreables, como Liberty Reserve y bitcoin, insuflan nueva vida a la economía clandestina y permiten el rápido intercambio de bienes y servicios. Con estos ingresos adicionales, Crimen, S. A. se está volviendo más disciplinada y organizada que nunca, y la sofisticación de sus operaciones aumenta sin cese. Los modelos de negocio se automatizan en la medida de lo posible para maximizar los beneficios, y las *botnets* pueden amenazar el comercio global legítimo, pues es posible entrenarlas para atacar a cualquier objetivo que Crimen, S. A. se fije. En su esencia, el mal ya está hecho. La máquina informática de delinquir en Internet ya se ha construido. Con estos sistemas en funcionamiento, la profundidad y el alcance global del poder de Crimen, S. A. implican que los delitos aumentan, y que lo hacen de manera exponencial. Sin embargo, por nefasta que sea esta amenaza hoy en día, está a punto de devenir mucho peor, a medida que, al adentrarnos en la era de la computación ubicua y la Internet de las Cosas, pongamos en manos de Crimen, S. A. miles de millones de objetivos nuevos para atacar.

Capítulo 12

Todo es pirateable

> Aún estamos en los primeros minutos del primer día de la revolución de Internet.
>
> SCOTT COOK, *Intuit*

Incluso en la era de Internet, comprar un coche puede ser un proceso laborioso, caro y frustrante. Peor si cabe si uno está desempleado o dispone de recursos limitados. Por suerte, el concesionario Texas Auto Center de Austin va dirigido específicamente a estos clientes y promete un automóvil para todo el mundo, «tanto si se tiene un presupuesto holgado como uno ajustado, si se está en la bancarrota, en plena expropiación de bienes o no se dispone de crédito alguno». Lógicamente, en tiempos de vacas flacas, la gente se retrasa en sus pagos de créditos y las tasas de expropiación en algunos concesionarios se elevan hasta un 45 por ciento. Un embargo nunca es divertido, ni para quienes están a punto de perder su medio de transporte principal ni para los vendedores, que tienen que enviar una flota de grúas en busca del automóvil. Quienes afrontan una expropiación suelen ocultar sus vehículos. Cuando la persona encargada de llevárselo se presenta con su grúa, los ánimos se inflaman y se sabe de embargantes que han recibido puñetazos, patadas, escupitajos, mordiscos, puñaladas e incluso balazos mortales por intentar recuperar la propiedad del concesionario. Sin duda, tenía que haber un planteamiento mejor… y en Texas Auto Center estaban convencidos de haber dado con la solución.

El concesionario adquirió una nueva herramienta tecnológica a la empresa Pay Technologies, con sede en Cleveland, herramienta que prometía ser una alternativa muy superior a los polémicos embargos del pasado. El producto de Pay Technologies recibía el nombre de WebTeckPlus y era un sistema que permitía a los concesionarios de automóviles instalar «una pequeña caja negra, del tamaño de una baraja de cartas, inteligentemente escondida bajo el salpicadero del vehículo». Estos dispositivos se controlaban de manera remota mediante un sitio web central que transmitía señales a través de una red inalámbrica a las cajas negras de los vehículos. Al activarse, la señal permitía al concesionario «desactivar el sistema de encendido del vehículo o activar el claxon para que empezara a sonar», un buen modo, sutilezas aparte, de recordar a los propietarios que iban retrasados en los pagos. De manera paulatina, Texas Auto Center empezó a instalar las cajas en toda su flota y al poco tiempo ya había mil cien vehículos con el sistema en activo. El encargado de administrar el nuevo sistema de embargo de alta tecnología era Omar Ramos-Lopez, un joven

ejecutor hipotecario del concesionario amante de la tecnología.

Todo parecía ir como la seda con el nuevo sistema hasta que, en febrero de 2010, de repente, unos cuantos vehículos de clientes de Texas Auto Center dejaron de funcionar de repente y no arrancaban. Los clientes no tenían ni idea de qué sucedía. Los libros de la empresa indicaban que los clientes estaban al corriente de sus pagos. A lo largo del día, el número de quejas fue en aumento y, al quinto día, más de cien propietarios habían irrumpido en el concesionario con sus reclamaciones airadas. ¿Qué diantres sucede?

Clientes a todo lo ancho y largo de Texas veían como, de súbito, sus vehículos quedaban inmovilizados y se negaban a arrancar. De manera aleatoria, en plena noche, los cláxones empezaron a sonar sin control por toda la ciudad de Austin y la policía registró numerosas quejas por ruido. Cuando los agentes llegaban al lugar, descubrían que el único modo de acallar los cláxones era desconectarlos físicamente de los cables de la batería del vehículo. Peor aún, aquellos centenares de clientes se encontraron sin transporte y se vieron obligados a ausentarse de sus puestos de trabajo, pese a que necesitaban desesperadamente cobrar.

Si bien al principio se restó importancia al incidente catalogándolo de «fallo mecánico sistémico», lo cierto es que había en juego algo mucho más perverso. Un intruso había accedido de manera ilegal al sistema de inmovilización de vehículos remoto mediante la web de Texas Auto Center y, uno a uno, había empezado a desactivar los automóviles de toda la ciudad. Los intentos del concesionario de volver a activar los vehículos fueron en vano porque, además, el *hacker* había modificado los registros en la base de datos, había cambiado los números de identificación de los automóviles y había reemplazado los nombres de los clientes legítimos por otros de personas famosas, como el del fallecido rapero Tupac Shakur y la cantante pop Jennifer López.

Era evidente que no encajaba y, con el tiempo, las sospechas recayeron en el veinteañero Omar Ramos-Lopez, a quien habían despedido del concesionario días antes de la parálisis vehicular generalizada por «no satisfacer los estándares de la empresa». Los agentes de policía alegaron que Ramos-Lopez había utilizado los conocimientos acerca del sistema de su antiguo empleador y la contraseña de otro extrabajador para vengarse por su despido desactivando vehículos en masa por todo Austin. La investigación policial demostró que el antiguo ejecutor hipotecario había iniciado la sesión en los servidores de Pay Technologies en Ohio desde una red de banda ancha de AT&T que conducía a su hogar[1]. Ramos-Lopez fue arrestado y acusado de delito de ataque a un sistema informático.

En cuanto al concesionario Texas Auto Center, desde luego no es el único que decidió instalar esta tecnología de reclamadores de deuda remotos en sus vehículos; en la actualidad hay más de dos millones de automóviles que la incorporan. Sin embargo, tal como veremos más adelante, hay decenas de millones de vehículos en todo el mundo que pueden ser controlados de un modo u otro a través de Internet, y

miles más de ellos se añaden a la red de información global cada día. Con tales cajas negras instaladas en un número creciente de automóviles, cada vez está más claro que nuestros coches pueden tener más puertas traseras de las que creemos.

Donde habita lo inalámbrico

En la breve historia de la informática moderna, hemos acabado por concebir los ordenadores como cajas de diversos tamaños. En la década de 1950, un solo ordenador ocupaba todo un edificio. En los años setenta, el tamaño de un ordenador central o servidor se había reducido a las dimensiones de un frigorífico. En la década de 1980 surgieron los ordenadores de sobremesa personales y en la década de 1990 nació el ordenador portátil. Con el cambio de siglo, el uso de los teléfonos móviles hizo explosión y, en 2007. Steve Jobs había dado al mundo su iPhone, un pequeño pero potente ordenador de mano. Como siempre, la ley de Moore avanza implacable, si bien en el futuro muy cercano nuestro concepto de lo que constituye un ordenador saltará por los aires cuando las cajas que siempre han contenido el procesador desaparezcan y nos adentremos en el reino de la computación ubicua.

A diferencia de los escritorios estacionarios del pasado, la era del *posPC* augura un mundo en el que el procesamiento informático tendrá lugar en todos sitios y en todas las cosas. Ya nos hallamos en plena transición. Las ventas de ordenadores portátiles suplantaron a las de ordenadores de sobremesa en 2005 y, en 2015, el número de tabletas, como el iPad, vendidas en todo el mundo aventajará a las ventas de ordenadores de sobremesa y portátiles juntas[2]. En 2014 había en el planeta más teléfonos móviles en uso que personas[3]. Y no hay que olvidar que los teléfonos inteligentes y las tabletas de nuestros hogares tienen compañía, como son las consolas de juegos, los grabadores de vídeo digital, los descodificadores y los televisores inteligentes, todos ellos en red y conectados a Internet. Sin embargo, un paseo por los pasillos de cualquier comercio de electrodomésticos revela el despunte de una nueva tendencia. En estas tiendas y en Internet en general, todo un nuevo abanico de dispositivos digitales compiten por hacerse un hueco en las redes de nuestros hogares: cosas como termostatos, bombillas, altavoces, monitores para bebés y sistemas de seguridad activados por Internet. En conjunto, representan los primeros pasos de un nuevo paradigma de la computación que emerge con fuerza y se conoce como la Internet de las Cosas (IoT por sus siglas en inglés, de *Internet of Things*). Y cuando despegue de verdad, probablemente cambiará para siempre el mundo tal como lo conocemos.

El Pew Research Center define la Internet de las Cosas como «un entorno computacional global, envolvente, invisible, ambiental y conectado en red construido mediante la proliferación continuada de centros de datos masivos, bases de datos,

software, cámaras y sensores inteligentes en un tejido de información que se extiende por todo el mundo»[4]. El término lo acuñó en 1999 el investigador del MIT Kevin Ashton, quien, mientras trabajaba en un proyecto para Procter & Gamble, constató que «si todos los objetos de la vida cotidiana estuvieran equipados con identificadores y conectividad inalámbrica, dichos objetos podrían comunicarse entre sí y gestionarse mediante ordenadores. […] Si existieran ordenadores que supieran todo lo que se puede saber y usaran los datos que recopilasen sin nuestra ayuda, seríamos capaces de rastrearlo y contarlo todo y, con ello, reducir enormemente tanto los residuos como las pérdidas y los costes»[5]. El concepto de Ashton era tan simple como imponente, y tuvo una gran repercusión en los fabricantes y minoristas como Walmart, que mejoraron de manera espectacular su gestión de la cadena de suministros y recortaron los costes para los clientes. No obstante, en 1999 no existía aún la tecnología necesaria para convertir la Internet de las Cosas en una realidad, más allá de entornos muy controlados, como los almacenes de las fábricas. En la actualidad, la situación ha cambiado y una confluencia de avances ha permitido dar grandes saltos adelante en el mundo de la informática ubicua y ha permitido, por vez primera, la «incrustación generalizada de ordenadores en miniatura en objetos y su conexión a Internet mediante tecnología inalámbrica». De hecho, de acuerdo con la Semiconductor Industry Association, en 2004 los seres humanos producíamos ya más transistores que granos de arroz… y a un menor coste[6].

Gracias a los avances en los circuitos, en el *software* y en la miniaturización es posible construir una Internet de las Cosas cuyos dispositivos encajan a grandes rasgos en una de dos categorías: sensores o microcontroladores. Los microcontroladores son procesadores informáticos programables minúsculos, de sólo unos milímetros de anchura. Son chips informáticos ultrabaratos y consumen poquísima energía; algunos son tan pequeños como la cabeza de un alfiler, y pueden construirse y engastarse en un número infinito de dispositivos por apenas unos céntimos[7]. Estos dispositivos informáticos en miniatura sólo consumen milivatios de electricidad y, por consiguiente, pueden funcionar durante años con una batería diminuta o con un pequeño panel solar. Como resultado, ahora es posible crear «un servidor web que quepa sobre (o dentro) de la punta de un dedo por sólo un dólar»[8].

Estos microchips recibirán datos de una gama casi infinita de sensores, dispositivos minúsculos capaces de monitorizar cualquier cosa que pueda medirse y registrarse, incluidos temperatura, potencia, localización, cal en el agua, radiación, presión atmosférica, aceleración, rotación, fuerza magnética, altitud, sonido y vídeo. Este despliegue mundial de sensores nos permitirá percibir, analizar e interactuar con el mundo que nos rodea de una manera en el pasado humanamente imposible. Una vez recopilados, estos datos no permanecerán inactivos, sino que se procesarán mediante un sinfín de nuevos microcontroladores de la Internet de las Cosas similares a los mencionados más arriba (interruptores en miniatura, activadores, válvulas, servomotores, turbinas y motores), todos ellos capaces de interactuar de manera

autónoma con el mundo físico que los rodea. De manera que, por ejemplo, cuando un sensor detecte una temperatura o una presión excesivas en un gasoducto, el microcontrolador que reciba la información estará programado para reaccionar cerrando o desviando el flujo del gas natural y evitar una explosión catastrófica.

El crecimiento expansivo de la redes de datos inalámbricos de alta velocidad permitirá a estos sensores comunicarse con el mundo mediante distintos protocolos y tecnologías de comunicaciones, como Wi-Fi, banda ancha, sistema global para las comunicaciones móviles (GSM), acceso múltiple por división de código (CDMA), Bluetooth, identificación de radiofrecuencias (RFID), comunicación de campo cercano (NFC), ZigBee, Z-Wave y tendidos eléctricos. Pero no sólo se comunicarán con la Internet más amplia, sino también entre sí y generarán cantidades insondables de datos de máquina a máquina (M2M), que se almacenarán y procesarán a mayor velocidad y menor coste gracias a la computación en la nube y a sus capacidades de almacenamiento de datos casi ilimitadas. El resultado será un «entorno computacional global, envolvente, invisible y ambiental conectado en red» y siempre activo, un mero preludio del tsunami de cambios que nos aguarda.

Ahora bien, primero habrá que arreglar una cosa: el protocolo de comunicaciones básico que canaliza casi todo el tráfico en Internet. La médula espinal de la Internet de hoy en día se ejecuta sobre lo que se conoce como Protocolo de Internet versión 4 (IPv4). Esta arquitectura de las comunicaciones nos acompaña desde 1981 y proporciona en torno a 4300 millones de direcciones de red distintas, cada una de las cuales representa un dispositivo conectado. Cuando se introdujo el IPv4 a finales de la década de 1970, nadie habría imaginado que 4300 millones de direcciones serían insuficientes para satisfacer las demandas de las poquísimas grandes universidades y empresas que había conectadas a Internet a la sazón[9]. En cambio, hoy en día, lo impensable ha sucedido: se han agotado las direcciones de Internet. Tal como la metrópolis de Nueva York tuvo que crear nuevos prefijos por barrio cuando se quedó sin números telefónicos que empezaran por 212 para proporcionárselos a los residentes, lo mismo ha sucedido con Internet.

La respuesta de Internet a este problema es el IPv6, que suplantará al IPv4 y aumentará considerablemente el tamaño del espacio accesible mediante direcciones disponibles online. El nuevo protocolo resuelve este problema aumentando la longitud del «número telefónico» de 32 a 128 bits. Matemáticamente, el IPv4 sólo soporta unos 2^{32} o 4300 millones de conexiones. El IPv6, por su parte, es capaz de gestionar 2^{128} o 340.282.366.920.938.463.463.374.607.431.768.211.456 conexiones[10]. Las implicaciones de un número de tal longitud son alucinantes. Sólo hay 10^{19} granos de arena en todas las playas del mundo. Eso implica que el IPv6 permitiría a cada grano de arena contar con un billón de direcciones IP[11]. De hecho, el IPv6 permite usar tantas direcciones que cada átomo de nuestro planeta podría recibir una dirección única y, pese a ello, «aún nos quedarían direcciones suficientes

para servir otros cien planetas Tierra»[12]. Precisamente en la estela de estos cambios nacerá la Internet de las Cosas.

Para poner estos formidables números en perspectiva, podemos concebir la Internet actual metafóricamente como una pelota de golf del doble de su tamaño habitual y la Internet del mañana como una bola del tamaño del Sol[13]. Eso significa que, en los próximos años, no sólo estarán conectados a Internet todos los ordenadores, teléfonos y tabletas, sino también todos los vehículos, viviendas, perros, puentes, túneles, tazas, relojes de pared, relojes de pulsera, marcapasos, vacas, farolas, oleoductos, juguetes y latas de refresco. Pese a que en 2013 sólo había trece mil millones de dispositivos en línea, Cisco Systems calcula que en 2020 habrá cincuenta mil millones de cosas conectadas a Internet, con el consiguiente crecimiento exponencial ulterior[14]. Cuando todos esos dispositivos se conecten en línea y empiecen a compartir datos entre sí, comportarán impresionantes mejoras en materia de logística, eficiencia de los empleados, funcionamiento de las cadenas de suministros, consumo energético, servicio de atención al cliente y productividad personal.

Tal como se ha indicado previamente, la ley de Metcalfe establece que el valor de una red aumenta de manera exponencial con el número de nodos u ordenadores unidos a ésta. Cuando el IPv6 añada 340 undecillones (340 billones de billones de billones) de nuevos nodos potenciales a la red de información global, la explosión concomitante en valor económico será incalculable. El McKinsey Global Institute vaticina que la innovación que la Internet de las Cosas posibilitará en múltiples sectores aportará hasta 6,2 billones de dólares adicionales a la economía mundial en 2025[15]. Es posible que sea en la Internet de las Cosas donde encontremos el próximo Google, Facebook o Apple, y el número de sensores, dispositivos de consumo y sistemas de control industrial en línea ya ha sobrepasado al número de teléfonos móviles[16]. Los primeros participantes de la Internet de las Cosas, como Fitbit, Jawbone, Oculus Rift, Withings, Estimote y Sonos, se han hecho notar y han obtenido una buena valoración en los mercados. De hecho, una de estas empresas, la empresa de termostatos inteligentes Nest Labs, fue adquirida en 2014 por unos asombrosos 3200 millones de dólares sólo 854 días después del lanzamiento de su primer producto. Y, aunque sin duda hay mucho dinero por hacer en la Internet de las Cosas, es posible que sus implicaciones sociales superen a su impacto económico.

Imaginar la Internet de las Cosas

> La Internet de las Cosas es una manera de decir que más parte del mundo pasará a formar parte de la Red. […] Cada vez asimilamos más parte del mundo en el ordenador.

La Internet de las Cosas suena prometedora. Puesto que se incrustarán chips y sensores en objetos cotidianos, tendremos una información mucho mejor y nuestras vidas serán más cómodas. Así, por ejemplo, si tienes el despertador conectado a Internet, podrá acceder a tu calendario y leerlo. Sabrá dónde y cuándo es tu primera cita del día y será capaz de cruzar esa información con las últimas informaciones acerca del tráfico rodado. Si hay poco tráfico, te permitirá dormir diez minutos más; si, por el contrario, el tráfico es denso, podrías sorprenderte despertando antes de lo que esperabas. Y cuando suene el despertador, encenderá gradualmente las luces de tu casa, y quizá también activará la calefacción o abrirá el grifo de la bañera para prepararte el baño. La puerta electrónica de la caseta de tu mascota se abrirá automáticamente para que Fido corretee por el jardín en su primera visita de la mañana y, lo que es más importante, la cafetera empezará a preparar tu primera taza de café justo a tiempo. No tendrás que preguntarles a tus hijos si se han lavado los dientes: el chip incorporado a su cepillo enviará un mensaje a tu *smartphone* para avisarte de que lo han hecho. Y cuando salgas por la puerta, no tendrás que buscar las llaves; el sensor con luz del llavero te permitirá localizarlas en un radio de cinco metros en tu hogar. Será como si la era de *Los Supersónicos* hubiera llegado al fin.

Si bien el medidor de entusiasmo de la Internet de las Cosas ha estado parpadeando en rojo durante un cierto tiempo, todo lo descrito arriba ya es técnicamente factible hoy. Para ser sinceros, habrá obstáculos, sobre todo relacionados con la falta de estándares técnicos comunes, pero una amplia variedad de empresas, consorcios y organismos gubernamentales están trabajando con denuedo para hacer de la Internet de las Cosas una realidad. El resultado será la transición de la conectividad a la hiperconectividad y, como todo lo relacionado con la ley de Moore, llegará a nosotros antes de que nos demos cuenta. La computación ubicua afectará a todas las áreas de las empresas humanas, incluidas entre ellas el transporte, la energía, las finanzas, el gobierno, la agricultura, la educación, la seguridad pública, los viajes y el comercio.

La Internet de las Cosas implica que, en el futuro, todos los objetos físicos llevarán asignada una dirección IP y se transformarán en tecnologías de la información. Así, tu lámpara, tu gato o tu ficus serán parte de la red de TI. Cosas que en el pasado eran silenciosas estarán ahora dotadas de voz, y cada objeto será capaz de narrar su propia historia y pasado. El frigorífico sabrá exactamente cuándo fue fabricado, los nombres de quienes lo construyeron, en qué fábrica y qué día salió de la cadena de montaje, llegó al minorista y pasó a formar parte de la red de tu hogar. Guardará un registro de cada vez que se ha abierto su puerta y sabrá a cuál de tus hijos se le ha olvidado cerrarla. Cuando el motor del frigorífico empiece a fallar, emitirá una señal para que lo revises y, cuando finalmente muera, te indicará cómo desmontarlo en piezas y el mejor modo de reciclarlas. Los edificios sabrán todas las

personas que han trabajado en ellos, las viviendas guardarán nota de todas las personas que las han habitado y las farolas sabrán exactamente qué coches han conducido junto a ellas.

Todos estos objetos se comunicarán entre sí y tendrán acceso al poder de procesamiento y almacenamiento masivos de la nube, que se verá incluso más potenciado por las redes móviles y sociales adicionales. Viviremos en un mundo donde todo es programable e interactivo. Los objetos se volverán «inteligentes» y serán capaces de indicar su ubicación, proximidad, velocidad, temperatura, flujo, aceleración, sonido ambiental, visión, fuerza, carga, par de torsión, presión e interacciones. Las primeras generaciones de teléfonos inteligentes, medidores inteligentes, relojes inteligentes y tarjetas inteligentes ya están entre nosotros, pero, en el futuro, todos los objetos serán inteligentes, mucho más inteligentes, de hecho, de lo que lo son hoy en día. A medida que los dispositivos se conecten en red, desarrollarán su propia forma limitada de conciencia, lo cual dará lugar a un mundo en el que las personas, los datos y las cosas estarán unidos. Como consecuencia del poder de la computación incrustada, veremos «miles de millones de "cosas" inteligentes y conectadas» uniéndose a una red neuronal mundial en la nube que «abarcará todos y cada uno de los aspectos de nuestras vidas»[17].

Mientras que la «vieja» Internet permitía que los ordenadores de sobremesa, los portátiles y los servidores compartieran información, la «nueva» Internet posibilitará controlar de manera remota cualquier objeto sobre la Tierra. Tal como explica Joi Ito, director del Media Lab del MIT, se está produciendo un «fenómeno de convergencia en el que bits del ámbito digital se están fusionando con átomos en el mundo físico»[18]. Cada objeto tendrá una identidad y una vida tanto en los mundos físico como virtual y, cuando esto ocurra, la diferencia entre estar en línea y fuera de línea, que en el pasado era significativa, desaparecerá. En este sentido, el director ejecutivo de Cisco, John Chambers, predijo recientemente que la Internet de las Cosas tendría un impacto entre cinco y diez veces más potente que la Internet que conocemos.

En este mundo, lo incognoscible se vuelve repentinamente cognoscible. Por ejemplo, será posible controlar el recorrido de las frutas y hortalizas desde los campos hasta la mesa, y los restaurantes podrán marcar cada plato, de tal modo que sabrán qué contenía, quién se lo ha comido y cuánto tiempo tardó en llegar desde la cocina hasta el comensal. Así, cuando se produzca un brote de *E. coli*, no será necesario cerrar quinientos restaurantes y preguntarnos si la causa fue el pollo o la ternera. Sabremos exactamente con qué restaurante, proveedor y comensal contactar para resolver el problema de manera rápida. La Internet de las Cosas y sus miles de millones de sensores crearán una red de inteligencia ambiental que piense, sienta, note y realice profundas aportaciones al universo cognoscible.

No sólo lo incognoscible deviene cognoscible, sino que lo imposible deviene súbitamente posible. Las cosas que solían tener sentido dejarán de tenerlo, como los detectores de humo. ¿Por qué los detectores de humo se limitan a emitir pitidos

agudos si tu vida está en peligro mortal debido a un incendio? En el futuro, encenderán las luces de la habitación para despertarte, encenderán tu equipo de música y reproducirán un archivo MP3 de audio que avise a gritos: «Fuego, fuego, fuego». También contactarán con los bomberos, llamarán a tus vecinos (por si has quedado inconsciente o necesitas ayuda) y desconectarán automáticamente todos los electrodomésticos de tu vivienda que funcionen con gas. Y no serás el único a quien la Internet de las Cosas salve la vida: también se la salvará a tus plantas[19]. Desde 2009 se utilizan unos sensores de humedad baratos que se colocan en la tierra de las plantas de casa y se conectan a redes Wi-Fi para enviar tuits en los que imploran: «¡URGENTE! ¡Riégame!».

¿No te parece lo suficiente futurista? ¿Qué opinas de una Internet de interespecies, una red que una a elefantes, delfines y simios con «fines de enriquecimiento, investigación y conservación»[20]? Aunque te pueda sonar a chifladura, ya está en marcha. En Australia, por ejemplo, hay más de trescientos tiburones en Twitter (y no, no crearon ellos la cuenta). Los investigadores colocaron etiquetas acústicas en 338 tiburones, las cuales emiten una señal a los receptores instalados en las orillas cuando los animales se encuentran a menos de un kilómetro de la playa[21]. En un país que ha sufrido más ataques de tiburón letales que ningún otro, este desarrollo de la Internet de las Cosas está salvando vidas humanas; no en vano, cerca de cuarenta mil bañistas se han suscrito como seguidores de las cuentas en Twitter de estos tiburones.

El producto derivado de la Internet de las Cosas será una red de información global viva, una red que respire, y la tecnología cobrará vida de modos hasta ahora sólo vistos en las películas de ciencia ficción. Y si bien este futuro puede antojarse muy remoto, las comunicaciones M2M (entre máquinas) ya han sustituido todas las actividades online originadas por humanos[22]. En 2013, más del 61,5 por ciento del tráfico mundial de Internet lo generaban ya cosas. A medida que nos internemos por la senda que conduce a la computación ubicua, es probable que los resultados y las implicaciones de este fenómeno nos alucinen. De la misma manera que la llegada de la electricidad en su día fue asombrosa, con el tiempo quedó relegada a un segundo plano y la electricidad se convirtió en un medio imperceptible y omnipresente con el que interactuamos de manera constante en el mundo físico[23]. Antes de que dejemos que esto ocurra y habida cuenta de las múltiples promesas de la Internet de las Cosas, debemos formularnos interrogantes esenciales acerca de este nuevo mundo que nos aguarda. Si bien sus numerosos beneficios parecen manifiestos, una Internet de todo también plantea un riesgo tremendo, puesto que de la misma manera que la electricidad puede provocar descargas y matar, también podrán hacerlo los miles de millones de cosas conectadas en red online.

Conectarlo todo… sin seguridad

La conexión de los productos a la Red será la electrificación del siglo XXI.

MATT WEBB, CEO, Berg Cloud

Para que las cosas puedan conectarse en línea y comunicarse entre sí, primero hay que dotarlas del equivalente tecnológico al habla. Tal como vimos en el caso del concesionario Texas Auto Center y tecnologías como la caja negra WebTeckPlus, podría decirse que los automóviles de hoy en día ya «hablan», y con sus graznidos revelan datos acerca de su localización, condición y estado. Para hacer realidad la visión esbozada por los defensores de la Internet de las Cosas es vital otorgar a los objetos cotidianos la capacidad de comunicarse con nosotros y entre sí.

Para que esto ocurra, la Internet de las Cosas recurre a una serie de tecnologías y protocolos de comunicación conflictivos. Desde la distancia, los estándares de transmisión de datos móviles como LTE (Long Term Evolution o Evolución a Largo Plazo), 4G, GSM y CDMA conectarán dispositivos con la red de telefonía móvil. Muchos objetos de mayor tamaño podrán comunicarse mediante las líneas de telefonía por cable fijas, como Ethernet y la fibra óptica, pero quizá por precio y practicidad la mayor parte de las conexiones tendrán lugar a través de redes inalámbricas. El resultado será la inclusión de miles de millones de chips en objetos que utilicen tecnologías estándares como Wi-Fi, Bluetooth, ZigBee, Z-Wave, comunicación de campo cercano (NFC) e identificación por radiofrecuencia (RFID) para comunicarse. A medida que el precio de estas herramientas descienda, nuevos productos de consumo como el iBeacon de Apple y las etiquetas de localización de Tile pasarán a ser una característica omnipresente en nuestras vidas cotidianas que nos permitirá rastrear objetos con una precisión de centímetros.

La primera de las tecnologías que permitirá la Internet de las Cosas, RFID, se patentó en 1983 y se trata de un dispositivo inalámbrico de bajo consumo que puede engastarse en cualquier objeto para convertirlo en «inteligente» o capaz de interactuar con lectores RFID. Las etiquetas RFID son circuitos electrónicos impresos del grosor de un trozo de papel que acostumbran a presentarse en formato de pegatina, no suelen medir más de 25 milímetros y pueden producirse por menos de un céntimo. Son capaces de intercambiar datos de manera constante y en tiempo real y pueden ser leídas por escáneres situados en un radio de cien metros. Incluso aunque no estés familiarizado con la tecnología RFID, es bastante probable que te hayas tropezado con ella en tu vida, ya sea en la tarjeta de identificación de seguridad con la que accedes a tu despacho, en tu tarjeta electrónica con chip inalámbrico, en la llave de tu habitación de hotel, en el pase del metro o en la pequeña caja que utilizas para pagar los peajes de las autopistas, como el E-ZPass. Pese a que la practicidad de la RFID, considerada por muchos la puerta de acceso a la Internet de las Cosas, suena

fenomenal, existe un pequeño problema: es claramente pirateable.

Se han detectado docenas de vulnerabilidades en las tecnologías RFID, cuya electrónica puede manipularse, burlarse y sobrecargarse fácilmente, y existe una «clandestinidad de la RFID» que trabaja con denuedo en mejorar de continuo sus técnicas ofensivas[24]. La abrumadora mayoría de las etiquetas RFID actuales no están dotadas de protocolos de seguridad, encriptación o privacidad seguros. Estas carencias han permitido al *hacker* de la seguridad Francis Brown construir sus propios lectores RFID, que vende por menos de cuatrocientos dólares y son capaces de escanear, copiar, clonar y robar datos de tus tarjetas inteligentes[25]. En consecuencia, mientras haces cola en la verdulería del barrio, viajas en un vagón de metro, subes en ascensor a la oficina o esperas a que te sirvan el primer café de la mañana en una cafetería Starbucks, Brown puede realizar un ataque «de cepillado». Mientras permanece de pie, con una sonrisa en el rostro y quizá te da conversación, el lector de RFIP portátil que lleva escondido en la mochila puede contactar con la tarjeta de la llave de tu oficina que llevas en el bolso, en el billetero o en un bolsillo y birlarte los datos codificados en ella. ¿Y qué problema hay?

Pues el siguiente: Brown puede conectar a continuación su lector de RFID al ordenador de su hogar y utilizarlo para clonar tarjetas RFID durante todo el día. Eso implica que puede colarse en tu oficina, habitación de hotel o vivienda cuando quiera. Todas las empresas Fortune 500 de Estados Unidos utilizan RFID en las placas identificativas de sus empleados para controlar el acceso a sus edificios de oficinas y Brown ha logrado una tasa de éxito del cien por cien clonando dichas tarjetas[26]. Las implicaciones que esto tiene en todos los aspectos, desde el espionaje industrial hasta el robo común o la seguridad de los empleados son enormes. Utilizar tarjetas de identificación RFID como sistema principal para garantizar la seguridad y la comprobación de identidad en el lugar de trabajo conlleva que el sistema actual es absolutamente inservible. Y lo que es peor, esas tarjetas no pueden actualizarse como el ordenador de tu hogar, descargando la última versión de *software*. Sería preciso sustituirlas todas, una reposición con un alto coste para una empresa con cien mil empleados.

Incluso aunque no utilices una tarjeta RFID para acceder a tu puesto de trabajo, hay muchas posibilidades de que ya o pronto la tengas engastada en la tarjeta de crédito de tu billetero. Los *hackers* también han demostrado ser capaces de vulnerarlas utilizando lectores de RFID baratos disponibles en eBay por sólo cincuenta dólares, herramientas que permiten a un atacante capturar de manera inalámbrica el número de tarjeta de crédito de su objetivo, así como la fecha de caducidad y el código de seguridad. Segundos después, mediante una herramienta de magnetización de tarjetas de trescientos dólares, los datos se codifican en una nueva tarjeta, con la cual es posible efectuar compras fraudulentas en un proceso que puede completarse en cuestión de minutos[27]. Bienvenido a los robos de cartera 2.0, donde los carteristas ni siquiera necesitarán meterte la mano en el bolsillo.

Las técnicas para piratear RFID son fáciles de emular y hay centenares de sitios de instrucciones y vídeos colgados en Internet en los que piratas informáticos explican cómo hacerlo punto por punto. Inquietante, cuando menos, dado que miles de millones de cosas que empiezan a conectarse a Internet utilizarán RFID como lenguaje principal para comunicarse e interactuar con el mundo. Además, los chips RFID pueden infectarse con virus, de la misma manera que es posible sobrecargar los RFID que funcionan con señales de GPS, lo cual te impedirá llegar a tu oficina y posibilitará a los ladrones robar productos caros etiquetados electrónicamente por los minoristas[28]. Otra tecnología popular de la Internet de las Cosas es la hermana menor de las RFID, conocida como comunicación de campo cercano (o NFC por sus siglas en inglés), en la actualidad incorporada en el 20 por ciento de los teléfonos móviles, sobre todo modelos Android y también los últimos dispositivos iPhone 6.[29] La NFC tienen múltiple usos, pero uno de los más habituales son los servicios de pago mediante móvil como Google Wallet.

Basta con deslizar el teléfono por encima de un lector de NFC para pagar un producto y su precio se deducirá del monedero virtual de tu teléfono o se cargarán en la tarjeta de crédito. Ahora bien, al igual que la RFID, la NFC ha sido vulnerada en múltiples ocasiones, gracias a aplicaciones de pirateo como NFCProxy, capaces de copiar datos de tarjetas de crédito NFC en tiempo real y reproducirlos después cuando los malhechores los utilicen para adquirir bienes y servicios de su elección[30]. Google Wallet también ha sufrido repetidos ataques de pirateo, incluidos entre ellos la lectura de tu PIN sin autorización y el acceso a los fondos almacenados en tu teléfono[31]. Y ahora que tu iPhone permite pagos móviles mediante Apple Pay, es probable que los delincuentes concentren su atención en vulnerar también el sistema de seguridad de Apple.

En otro ejemplo, un *hacker* atacó con éxito el chip de NFC de un teléfono móvil cercano para hacerse con el mando del dispositivo y efectuar llamadas telefónicas, enviar mensajes de texto y acceder a archivos, todo ello sin que el verdadero propietario del dispositivo se diera cuenta[32]. Ya se están utilizando aplicaciones NFC en teléfonos móviles para pagar en sistemas de tráfico locales, y timadores en San Francisco y Nueva Jersey han pirateado las cabinas de peaje con NFC mediante una aplicación llamada UltraReset, que reintegra automáticamente cualquier cargo deducido por operadores de trenes, lo cual equivale a viajar en metro gratis de por vida[33].

Otra tecnología de comunicaciones inalámbrica de la Internet de las Cosas cuyo uso y popularidad se han disparado es Bluetooth, si bien, al igual que la RFID y la NFC, es muy fácil subvertirla. Hay docenas de aplicaciones y programas gratuitos como Blue Scanner, Blue Bugger, BT Browser y Blue Sniff que simplifican a cualquier individuo con malas intenciones conectarse a un dispositivo dotado con Bluetooth y hacerse con su control. Estas herramientas proporcionan un acceso no autorizado (bautizado como *bluesnarfing*) a través del puerto de Bluetooth a todos los

datos almacenados en teléfonos móviles, ordenadores de sobremesa y ordenadores portátiles. También pueden interceptar los datos que tecleas en teclados inalámbricos, leer tus mensajes de texto, hacer fotografías sin tu conocimiento e incluso escuchar a hurtadillas a través de tus auriculares Bluetooth mientras permaneces sentado en el aeropuerto a la espera de que despegue tu avión[34].

Ya tenemos encima la fiebre del oro de la Internet de las Cosas y no hay marcha atrás. Pese a que conectarlo todo a la Internet de las Cosas global puede tener de hecho un valor tremendo, conectarlo todo de manera insegura no lo tiene. Antes de que añadamos miles de millones de cosas pirateables y nos comuniquemos mediante protocolos de transmisión vulnerables debemos formularnos preguntas importantes acerca de los riesgos concomitantes con relación a las implicaciones exponenciales para el futuro de la seguridad, los delitos, el terrorismo, la guerra y la privacidad.

El fin de la privacidad

> Objetos de interés serán localizados, identificados, monitorizados y controlados de manera remota mediante tecnologías como la identificación de radiofrecuencias, redes de sensores, servidores diminutos incrustados y recolectores de energía, todos los cuales se conectarán a la Internet de la siguiente generación mediante una computación abundante, de bajo coste y alta potencia.
>
> DAVID PETRAEUS, director de la CIA (jubilado)

De la misma manera que hoy en día es posible rastrear, grabar, vender y monetizar todos nuestros movimientos en Internet, en el futuro cercano también será posible hacerlo en el mundo real. El espacio real pasará a ser igual que el ciberespacio y, cuando todos los objetos de nuestro alrededor pasen a formar parte de la Internet de las Cosas, toda distinción significativa entre los mundos en línea y fuera de línea se desvanecerá.

Con la adopción generalizada de más dispositivos en red, lo que las personas hagamos en nuestros hogares, vehículos, lugares de trabajo, escuelas y comunidades estará sujeto a una supervisión y un análisis mayores por parte de las empresas que fabrican estos dispositivos. Desde luego, esos datos se revenderán a anunciantes, intermediarios y gobiernos por igual, y proporcionarán un acceso sin precedentes a nuestras vidas cotidianas. Por desgracia, al igual que nuestra información en las redes sociales, dispositivos móviles y datos de localización y financieros, nuestros datos en la Internet de las Cosas se filtrarán y proporcionarán mayores posibilidades a los acosadores y malhechores interesados en rastrearnos sin cesar. Pese a que sin duda sería posible establecer regulaciones y protocolos de seguridad para proteger a los consumidores de tales actividades, si el pasado puede servirnos de prólogo, lo más

probable es que cada dispositivo conectado a la Internet de las Cosas, ya se trate de una plancha, un aspirador, un frigorífico, un termostato o una bombilla, se proporcione con unas condiciones de servicio que garanticen a los fabricantes acceso a todos tus datos. Y lo más inquietante es que, pese a que teóricamente sería posible cerrar sesión en el ciberespacio, en tu hogar inteligente y conectado no habrá una cláusula de «exclusión voluntaria». Por consiguiente, más parte de lo que suceda tras las puertas cerradas quedará expuesto para su escrutinio por partes que nunca invitarías a tu casa, y en este mundo bajar las persianas no impedirá que seamos pasto de los mirones del siglo XXI[35].

Nos descubriremos interactuando con miles de objetos pequeños a nuestro alrededor a diario, cada uno de los cuales recopilará datos en apariencia inocuos las veinticuatro horas de los siete días de la semana, información que esos objetos comunicarán a la nube, donde será procesada, correlacionada y revisada. Tu reloj inteligente revelará que haces poco ejercicio a tu mutua sanitaria, tu vehículo comunicará a tu aseguradora que sueles saltarte el límite de velocidad y tu basura informará al ayuntamiento de que no estás acatando la normativa de reciclaje municipal. Ésta es la «Internet de los chivatos» y aunque puede sonar inverosímil, ya está sucediendo. Empresas de seguros automovilísticos como Progressive ofrecen tarifas personalizadas con descuento en función de tus hábitos de conducción. «Cuanto mejor conduzcas, más ahorras», anuncian. Lo único que los conductores han de hacer para disfrutar de una tarifa reducida es acceder a que le instalen la tecnología de caja negra Snapshot de Progressive en sus vehículos y permitir que controlen de manera continua sus frenadas, aceleración y kilometraje[36]. No obstante, no es irrazonable creer que, con el tiempo, los conductores que no accedan a que les instalen tales dispositivos en sus vehículos se enfrenten a primas atrozmente elevadas que conseguirán que *de facto* estas tecnologías devengan obligatorias.

La Internet de las Cosas proporcionará un amplísimo abanico de opciones a los anunciantes para que alarguen sus tentáculos hacia ti en cada uno de tus dispositivos inteligentes conectados. Eso implica que cada vez que abras la nevera para buscar hielo, se te presentarán anuncios de productos basados en los alimentos que tu frigorífico sabe que es más probable que adquieras. Además, las pantallas serán ubicuas, y los comerciantes ya están haciendo planes relativos a la abundancia de oportunidades que ofrecen para la publicidad. A finales de 2013, Google envió una carta a la Securities and Exchange Commission indicando que «nuestra empresa y otras podríamos [en breve] presentar anuncios y otro contenido en frigoríficos, salpicaderos de automóviles, termostatos, gafas y relojes, por mencionar sólo algunas posibilidades»[37]. Tenemos en cuenta que Google ya lee tu Gmail, registra todas tus búsquedas en la Red y lleva un seguimiento de tu localización física mediante tu teléfono móvil Android, ¿qué otras potentes incursiones en tu vida personal concebirá la empresa cuando su sistema de entretenimiento forme parte de tu vehículo, su termostato regule la temperatura de tu hogar y su teléfono de pulsera inteligente

supervise tu actividad física?

La RFID y otras tecnologías de comunicación de la Internet de las Cosas rastrean otros objetos inanimados, pero en el futuro se utilizarán también para hacer un seguimiento de seres vivos. Muchas personas con mascota ya están familiarizadas con empresas como PetLink, HomeAgain y AKC Reunite, que proporcionan chips RFID implantables a los veterinarios para que los perros y gatos perdidos puedan ser identificados y devueltos a sus hogares si se escapan. Sin embargo, lo que posiblemente no se sepa es que cada vez son más los seres humanos a los cuales también se realiza un seguimiento forzoso a través de sistemas de pulseras RFID, como las que hoy ya se utilizan de manera corriente en las cárceles y penitenciarías desde Los Ángeles hasta Washington, D. C. En algunos países, como por ejemplo en el Reino Unido, el gobierno se está planteando implantar chips RFID directamente bajo la piel de los presos, como es ya una práctica habitual en los perros[38]. Y aunque muchas personas podrían no poner objeciones a que los delincuentes convictos estuvieran sujetos a este tipo de rastreo mediante RFID, sin duda pensarán de manera muy distinta cuando técnicas similares se apliquen a sus propios hijos.

Directivos de escuelas de todo Estados Unidos han empezado a engastar chips RFID en los carnets de identidad de los escolares y se exige a los alumnos que los lleven consigo en todo momento. En Contra Costa County, California, se requiere ya a los alumnos de preescolar que lleven camisetas de tirantes con dispositivos de rastreo incorporados que permiten al personal docente y administrativo saber exactamente dónde está cada alumno. Según los directivos de las escuelas del distrito, los sistemas RFID ahorran «3000 horas de trabajo al año invertidas en buscar y procesar a los estudiantes»[39]. Por supuesto, cuando las personas se ven obligadas a conectarse a la Internet de las Cosas, surgen una amplia variedad de interrogantes relacionados con las políticas públicas y de privacidad. Así por ejemplo, el mismo sistema RFID que permite controlar constantemente a los alumnos permitirá identificar a aquellos que se muevan «demasiado», los cuales podrían ser catalogados de hiperactivos, perturbadores y más idóneos para asistir a «escuelas alternativas». Y a los alumnos que no desean someterse a tal control sencillamente les espetarán un «¡Es lo que hay!»[40]. En 2013, la estudiante de segundo año de universidad Andrea Hernandez de San Antonio, Texas, fue expulsada por negarse a llevar su dispositivo RFID en el campus.

Entre tanto, rastrear a los empleados y saber cuánto tiempo se toman en la pausa para la comida, cuánto duran sus visitas al lavabo y el número de *widgets* que producen será pan comido. Es más, quedarán registradas incluso cosas como cuántas palabras se teclean por minuto, los movimientos oculares, el total de las llamadas respondidas, la respiración, el tiempo de ausencia del escritorio y la atención al detalle. El resultado será un entorno de trabajo moderno que, si bien será más productivo, también se asemejará más a una cárcel. Ahora bien, no sólo tu empleador accederá a los datos en la Internet de las Cosas para contrastar tu eficiencia y

controlarte, pronto también lo hará el gobierno. Los cuerpos policiales ya solicitan a las empresas de suministros locales que revelen qué clientes tienen facturas eléctricas inusitadamente altas, las cuales relacionan con el cultivo de marihuana en casa. Basándose exclusivamente en esas facturas eléctricas se han emitido órdenes de registro y se ha arrestado a sospechosos[41]. En el futuro, los cuerpos de seguridad podrán saltarse por completo la citación y comprobar directamente de manera remota tu contador inteligente para saber si tu consumo de energía se «ajusta al perfil» de los hogares de tu vecindario o no.

En la escena de un crimen, la policía podrá interrogar al frigorífico y preguntarle el equivalente a: «¿Ha visto usted algo?». Los asistentes sociales de niños sabrán si durante la semana pasada la familia se quedó sin pañales y leche y lo único que había en el frigorífico eran cervezas. La Internet de las Cosas también inaugura el mundo del «cumplimiento de la ley a pies juntillas». Así, cuando haya sensores por doquier y todos los datos se rastreen y registren, es más probable que recibas una multa por exceso de velocidad por ir a 62 kilómetros por hora en una zona de 60 kilómetros por hora o que te multen por pasarte veinte segundos del tiempo indicado en tu tique de aparcamiento. Como ya han demostrado las cámaras de control fotográfico instaladas en los semáforos, cuando todo está conectado, es imposible ocultar nada, sobre todo si las infracciones se traducen en ingresos para los organismos gubernamentales y sus socios empresariales.

El exdirector de la CIA David Petraeus ha señalado que la Internet de las Cosas «transformará la clandestinidad»[42]. Mientras que el viejo modelo de espionaje gubernamental y empresarial podía implicar ocultar un micrófono bajo la mesa en la sala de conferencias para escuchar tus conversaciones, en el mañana esa misma información podrá obtenerse interceptando en tiempo real los datos que envíe tu bombilla Wi-Fi a la aplicación de iluminación de tu teléfono móvil. De este modo, los dispositivos que creías que trabajaban en tu beneficio de hecho podrían estar en nómina de otra persona o empresa, en especial de Crimen, S. A.

Piratería de *hardware*

Una raza mucho menos frecuente de *hackers* atacan los componentes físicos de tu sistema informático, entre los cuales se incluyen microchips, circuitos electrónicos, controladores, memoria, circuitería, componentes, transistores y sensores, elementos nucleares de la Internet de las Cosas. Estos piratas atacan el *firmware* del dispositivo, es decir, el conjunto de instrucciones informáticas, presente en todo dispositivo electrónico que encuentran, incluyendo televisores, receptores estéreo, teléfonos móviles, consolas de videojuegos, cámaras digitales, discos duros, impresoras, automóviles, aviónica, apartados de calefacción y aire acondicionado, enrutadores de

red, sistemas de alarma, circuitos cerrados de televisión (CCTV), sistemas de control industrial SCADA, memorias USB, semáforos, parquímetros, surtidores de gasolinera, relojes digitales, sensores, sistemas domóticos inteligentes, robótica y controladores lógicos programables (como los utilizados por los iraníes en Natanz). Esta cantidad abrumadora de objetos «inteligentes» son completamente «tontos» y es absolutamente imposible actualizar su *firmware*.

Es más, los pequeños ordenadores que integran la Internet de las Cosas y la mayoría de nuestros dispositivos electrónicos cotidianos tienen una potencia de procesamiento y una memoria muy limitadas. A causa de estas limitaciones, es preciso construirlos con acuerdo a unas especificaciones asombrosamente precisas que apenas permiten acomodar las funciones que los diseñadores necesitan introducir para que los dispositivos funcionen, lo cual deja un amplio y valioso espacio libre para algo tan «trivial» como la seguridad, a menudo una consideración de última hora en el proceso de fabricación. La mayoría de *firmware* carece de un mecanismo automático común para actualizarse y solucionar los problemas de funcionalidad o seguridad detectados después del envío del dispositivo, lo cual convierte a la mayoría de los dispositivos conectados a Internet desde hace entre cinco y diez años en presas fáciles. En el caso de algunos objetos más caros, como los *smartphones*, el *firmware* del dispositivo está diseñado para actualizarse, cosa que permite descargarse las mejoras y los parches de seguridad. Sin embargo, en el resto de dispositivos electrónicos, los fabricantes rara vez modifican el *firmware* a lo largo de su vida útil, pues para ello sería preciso reemplazar físicamente los circuitos integrados en el objeto, un obstáculo económico carísimo. No obstante, aunque tu teléfono incorpore el último *firmware* disponible, siempre hay peligros que deben tenerse en cuenta.

Si bien muchos usuarios de iPhone y Android entienden que descargarse la aplicación o el archivo informático erróneos puede infectar sus teléfonos con un virus, muy pocos, si es que existe alguno, saben que el cargador de su teléfono móvil también puede infectarlos. Los *hackers* ya han logrado crear un virus de *hardware* destinado directamente a un cargador USB vulnerable capaz de atacar dispositivos Apple. Y basta con conectar el teléfono a uno de los cables de alimentación corruptos para que se infecte[43]. Al modificar el *firmware* y la electrónica del pequeño e inocente enchufe que utilizamos para cargar nuestros teléfonos, los atacantes lograron sortear las barreras de seguridad del iPhone e infectar el teléfono. No se mostraba ningún mensaje de alerta y el *malware* que se ejecutaba de manera furtiva no aparecía visible en la lista de programas en ejecución. No obstante, en un segundo plano, el cargador corrupto instalaba una puerta trasera en el dispositivo que permitía a los *hackers* efectuar llamadas telefónicas, leer mensajes de texto, robar información bancaria, capturar las contraseñas de las cuentas y rastrear los movimientos de los usuarios de los teléfonos[44]. Este fenómeno se conoce con el nombre de *juice jacking* y el cargador infectado se montaba por menos de cincuenta dólares, dato que conviene que tengas en cuenta la próxima vez que conectes tu teléfono inteligente sin

batería a una estación de recarga en un aeropuerto, hotel o centro comercial (los lugares donde los *hackers* colocarían estos dispositivos con el fin de infectar al mayor número de víctimas posible).

Los cargadores modificados de manera ilegal no son las únicas sorpresas de *hardware* ante las cuales hemos de estar atentos. Prácticamente todo lo que lleve un microcontrolador o sensor puede llegar a tu hogar con «funciones mejoradas» que nadie querría para sí. En 2013 en Rusia, los funcionarios de aduanas se percataron de que una serie de productos al consumo fabricados en China, incluidas teteras eléctricas y planchas para ropa, llegaban con modificaciones que no complacían en absoluto a las autoridades rusas[45]. Los dispositivos contenían tarjetas Wi-Fi en miniatura ocultas capaces de propagar *software* malicioso a través de cualquier red de Internet abierta en doscientos metros a la redonda y eran capaces de «telefonear a casa» y enviar mensajes secretos a China[46]. Estas planchas y teteras no sólo eran capaces de unirse subrepticiamente a tu red Wi-Fi (algo que nadie esperaría nunca de una plancha normal y corriente), sino que podían utilizar tu propia red para propagar virus a otros ordenadores de tu hogar y diseminar mensajes de correo no deseado entre tus vecinos y el resto del mundo. Y aunque nos gustaría creer que las planchas espías y los cargadores de iPhone pirateados son rarezas, la realidad es que ya hay indicios de amenazas mucho más graves y generalizadas planteadas por la rápida asimilación de miles de millones de objetos conectados a la red de información mundial.

Cuantas más conexiones, más vulnerabilidades

Pese a los beneficios incalculables de la Internet de las Cosas, sus desventajas potenciales son colosales. La adición de cincuenta mil millones de objetos nuevos a la red de información global de aquí a 2020 implica que cada uno de estos dispositivos, para bien o para mal, será capaz de interactuar en potencia con los otros cincuenta mil millones de objetos conectados en la Tierra. El resultado serán 2,5 setillones de interacciones posibles de objeto a objeto conectado, una red tan extensa y compleja que apenas puede ser entendida o modelada. La Internet de las Cosas será una red mundial de consecuencias imprevistas y eventos de Cisne Negro que hará cosas para las que no estaba concebida. Si bien una red de tales características puede tener beneficios fortuitos, también hay muchas posibilidades de que registre desarrollos indeseados que afecten negativamente a la seguridad mundial, la privacidad personal y los derechos humanos[47]. Es más, si crees que el número de mensajes de error y bloqueos de aplicaciones que afrontamos hoy en día es un problema, espera a que la Red esté engastada en todos los objetos, desde tu automóvil

hasta tus zapatillas deportivas y tu microondas. Tener que reiniciar el frigorífico, el termostato y la puerta del garaje para que funcionen tampoco será demasiado agradable.

Si ha existido alguna vez una tecnología que encarnara el efecto mariposa, sin duda alguna es la Internet de las Cosas. En este mundo es imposible conocer las consecuencias de conectar la batidora de tu hogar con la misma red de información que una ambulancia de Tokio, un puente de Sídney o una cadena de montaje de un fabricante automovilístico de Detroit y, sin embargo, de uno u otro modo estarán conectados.

Mientras que algunas de las empresas de investigación y tecnología más clarividentes del mundo se apresuran a adentrarse en la Internet de las Cosas (y reclaman su parte en su bonanza económica multibillonaria), sus colegas en el Departamento de Seguridad del TI trabajan frenéticamente por combatir el ataque del día cero o la vulnerabilidad de *malware* del día. Apenas queda tiempo para especular y prepararnos para lo que viene. Los inmensos niveles de ciberdelincuencia a los que hacemos frente hoy en día dejan suficientemente claro que somos incapaces de proteger de manera adecuada los ordenadores de sobremesa y portátiles estándares que ya tenemos conectados en línea, por no hablar de los centenares de millones de teléfonos móviles y tabletas que incorporamos año tras año. ¿En qué visión de futuro, por consiguiente, es concebible que sepamos cómo proteger los siguientes cincuenta mil millones de cosas que se conectarán en red? A tenor de la incapacidad para manejar con seguridad la matriz de información mundial de hoy en día, ¿qué nos invita a pensar que seremos capaces de proteger un mundo en el que todas las cosas, desde las mascotas hasta los marcapasos pasando por los automóviles con piloto automático, estarán conectadas a la Red y podrán piratearse desde cualquier lugar del planeta? La realidad palmaria es que somos incapaces de hacerlo.

La Internet de las Cosas se convertirá en la Internet de las Cosas Pirateables, el colmo de la abundancia de oportunidades de llevar a cabo fechorías para aquéllos con los medios y la motivación necesarios para aprovecharse de nuestra inseguridad tecnológica habitual. La Internet de las Cosas y los protocolos inseguros subyacentes a ésta abrirán una caja de Pandora de vulnerabilidades en materia de seguridad a una escala sin precedentes y con el potencial de generar fallos de funcionamiento sistémicos cuyo alcance será impredecible, extraordinario y aterrador.

¡Houston, tenemos un problema! Sobre todo, con la superficie de la amenaza, es decir, con la suma de los diferentes vectores o puntos de ataque desde los cuales el enemigo puede golpearnos. El desafío de la Internet de las Cosas es que nuestra superficie de amenazas tecnológicas crece de manera exponencial y, por decirlo simple y llanamente, no tenemos ni idea de cómo defenderla de manera eficaz. La lógica es clara: cuantas más puertas y ventanas tengas, por más puntos puede colarse un caco en tu hogar, sobre todo en un hogar conectado a Internet.

Capítulo 13

Hogar, pirateado hogar

> Calculamos que actualmente sólo el uno por ciento de las cosas que podrían tener una dirección IP la tienen; de ahí que nos guste afirmar que el noventa y nueve por ciento del mundo aún dormita. Sólo nuestra imaginación puede proyectar qué sucederá cuando ese noventa y nueve por ciento se despierte.
>
> PADMASREE WARRIOR, director de tecnologías, Cisco

Blake Robbins, un estudiante del Lower Merion School District de Pensilvania, no atinaba a imaginar por qué lo habían convocado al despacho del director. Cuando la subdirectora acusó al alumno de dieciséis años de «comportamiento indebido», Robbins alegó que no tenía ni idea de qué le hablaban. La subdirectora se lo aclaró: sabía que el alumno tomaba drogas y lo amenazó con expulsarlo de la escuela. El adolescente negó con vehemencia las alegaciones, hasta que, de repente, la subdirectora volvió hacia él su ordenador portátil y mostró a Robbins varias fotos en las que aparecía *en su propio dormitorio* sosteniendo unas pequeñas pastillas de forma oblonga en la mano que procedía a ingerir. Atónito, el chaval preguntó de dónde habían salido aquellas fotos, aspecto que la subdirectora consideró irrelevante aclarar.

Robbins regresó a su casa y les relató el incidente a sus padres, quienes decidieron exigir explicaciones a la escuela pública. Resultó ser que Robbins ni consumía ni traficaba con drogas, sino que sencillamente había comido unos caramelos de color rojo de la marca Mike and Ike, como bien sabían sus padres. Pero ¿cómo diantres había conseguido el personal de la escuela obtener una fotografía del chaval de dieciséis años en su propio dormitorio comiendo caramelos? Mediante un complejo programa de espionaje supuestamente concebido para proteger las propiedades de la escuela.

Los funcionarios de la escuela municipal de aquel distrito pudiente habían proporcionado a 2300 alumnos de secundaria ordenadores portátiles MacBook para potenciar sus estudios. Ahora bien, lo que se abstuvieron de revelar tanto a los estudiantes como a los progenitores de éstos fue que esos ordenadores llevaban instalado un *software* secreto que ofrecía a los administradores acceso remoto a todas las actividades que los alumnos realizaban en los dispositivos, incluidos registros de chats entre alumnos e informes de los sitios web que visitaban. Además, el *software* les permitía también accionar de manera remota la cámara del portátil para fotografiar y grabar a los alumnos cuando los dispositivos estaban abiertos, todo ello, supuestamente, para llevar un seguimiento de los portátiles robados o perdidos. El

sistema de espionaje remoto estaba configurado para tomar fotografías instantáneas de manera tácita y automática cada quince minutos cuando el ordenador del alumno estaba abierto y encendido, si bien el personal escolar podía ajustar ese intervalo a sólo sesenta segundos en el caso de sospechar que algún estudiante presentaba un «comportamiento inadecuado».

Las fotografías se cargaban en el servidor web de la escuela municipal, donde funcionarios del distrito las revisaban una a una. Dichos funcionarios capturaron más de 56 000 imágenes, incluidas entre ellas fotografías de niños desnudos en sus dormitorios, cuartos de baño o cualquier otro lugar al cual hubieran acudido con sus ordenadores portátiles. De manera encubierta, los administradores habían tomado más de cuatrocientas imágenes sólo de Robbins desde que habían comenzado a sospechar de su comportamiento indebido, si bien no se lo notificaron a la policía y la escuela no solicitó ninguna orden de registro para realizar tales actividades invasivas. Una vez se hizo pública la noticia del indignante comportamiento de la escuela, se presentaron numerosas demandas legales, incluida la de los propios padres de Robbins, y el FBI inició una investigación criminal contra el distrito[1]. Tal como Robbins relató a *Good Morning America*: «Es como si hubieran estado sentados en mi dormitorio observándose sin que yo me diera cuenta»[2]. Por desgracia, en el momento en el que el estudiante de segundo año había recibido su portátil «gratuito», era demasiado joven para haber estudiado aún la advertencia profética acerca de los regalos de los griegos, un tema que probablemente entraría en el temario dos años después, cuando en sus clases de inglés avanzado la lectura fuera la *Eneida* de Virgilio.

Cámara cándida

> Hoy por hoy, vayas donde vayas, debes dar por supuesto que no tienes privacidad, porque los métodos de vigilancia son cada vez más asequibles e invisibles.
>
> HOWARD RHEINGOLD

Cuando una escuela pública, una institución estatal, está capacitada para espiarnos en nuestros hogares a su albedrío y sin orden judicial de por medio, es evidente que la era de la vigilancia universal ubicua ya ha llegado. Desde Londres hasta Nueva York, desde Chicago hasta Pekín, se han instalado redes de videovigilancia masiva o CCTV por todas partes para protegernos de amenazas, reales e imaginarias. Sólo en una ciudad, Chongqing, en el suroeste de China, el gobierno ha instalado quinientas mil cámaras para contener el malestar religioso y político, así como otros «delitos organizados»[3]. Pese a que antaño el gobierno tenía el monopolio sobre estos

sistemas de seguridad, en la actualidad podemos encontrar cámaras en fruterías, gasolineras, concesionarios de vehículos, hospitales, escuelas, edificios de oficinas, puentes, túneles, bares, taxis, autobuses, trenes, consultas médicas y lavanderías. También las incorporan nuestros ordenadores portátiles, teléfonos móviles, consolas de juegos, televisiones, tabletas, cámaras de vigilancia de bebés y sistemas de seguridad en el hogar, y, cuanto más ubicuas se vuelven, menos nos percatamos de su presencia. Dado el coste casi nulo de estos sensores de vídeo baratos, su presencia en nuestras vidas está a punto de ampliarse enormemente a medida que Internet desarrolle su propio sentido de la visión.

Las prestaciones y la calidad de las cámaras actuales están mejorando a niveles inimaginables y hace ya mucho tiempo que han dejado en la cuneta a las fotografías en blanco y negro con grano del pasado. El Departamento de Defensa de Estados Unidos ya ha desplegado una cámara de 1,8 gigapíxeles que puede acoplarse a un dron y detectar objetivos «de tan sólo 15 centímetros desde una altura de 20 000 pies» (tecnología que sin lugar a dudas estará disponible comercialmente en el futuro cercano[4]). Es más, las cámaras actuales no sólo observan y graban, sino que también pueden ver y entender, gracias a la asociación de sus sensores con algoritmos de computación en la nube y análisis de datos masivos. De manera que las cámaras son capaces de realizar reconocimiento facial, leer matrículas de vehículos e incluso determinar que un paquete (una bomba en potencia) se ha dejado descuidado en algún lugar durante demasiado tiempo[5]. Este análisis puede realizarse en tiempo real, y también de manera retrospectiva, lo cual posibilita desbloquear millones de horas de metraje de vídeo grabado tiempo atrás en busca de «una mujer con sombrero rojo».

Por desgracia, las herramientas concebidas para protegernos pueden generar una falsa sensación de seguridad, cuando centenares de millones de cámaras alrededor del mundo se conectan a la Red y resultan ser vulnerables a los ataques malintencionados de *hackers*. Tal como se ha analizado con anterioridad, la cámara de tu teléfono móvil puede activarse fácilmente a distancia sin que te des cuenta, mediante herramientas ampliamente disponibles como Mobile Spy (*software* del que ya se han vendido sesenta mil copias).

Una joven que aprendió esta lección por las duras fue Cassidy Wolf, Miss EE. UU. Adolescente, cuyo ordenador portátil abierto cayó bajo el control de un pirata informático que tomó fotografías y vídeos de desnudos de ella mientras paseaba por su dormitorio al salir de la ducha o se vestía para ir a la escuela[6]. Su atormentador la observó a diario durante varios meses hasta que un día le envió un mensaje de correo electrónico «sextorsionándola» y exigiéndole que realizara una serie de actos sexuales ante la cámara para él «o subiré estas fotografías y muchas otras (tengo MUCHAS otras y de mejor calidad) a todas tus cuentas para que todo el mundo te vea y, en vez de ser modelo, acabes siendo una estrella del porno [*sic*]». Al recibir aquella amenaza por correo electrónico, Cassidy cerró de un manotazo el portátil y rompió a llorar, antes de decidir acudir a la policía. Tres meses después, una

investigación del FBI reveló que uno de sus compañeros de clase en el instituto, Jared Abrahams, era el acosador. Abrahams perpetró su ataque utilizando Blackshades, un kit de herramientas de Crimen, S. A. a la venta en Crimenazon.com, *software* malicioso que utilizó para espiar a otras ocho mujeres en California del Sur[7].

Entre tanto, las cámaras de monitorización de bebés actuales, que permiten a los padres ver a sus retoños no sólo desde la habitación contigua, sino a través de Internet, son otro punto de presencia en la Red a la espera de ser vulnerado. Piratas y pedófilos suelen atacar de manera rutinaria estos dispositivos, la mayoría de los cuales no requieren contraseña o bien utilizan una estándar que proporciona el fabricante, cosa que posibilita la existencia de un espeluznante comercio de imágenes de cámaras de vigilancia de bebés en la clandestinidad digital, incluidas entre ellas las de jóvenes madres amamantando a sus hijos. Estas cámaras no sólo permiten realizar panorámicas completas, sino también ajustar el ángulo y ampliar o reducir la imagen, e incluyen audio bidireccional, gracias al altavoz y micrófono incorporados, que permiten a los padres escuchar y hablar a sus pequeños. Son muy prácticas para mamá, para papá… y también para el *hacker*, tal como descubrió Heather Schreck, de Cincinnati, cuando una madrugada se despertó de su sueño profundo.

«De repente escuché lo que sonaba como la voz de un hombre, pero estaba dormida, así que no estaba segura de haberla oído de verdad[8]» Confusa, Heather comprobó la cámara del vigilabebés del dormitorio de su hija de diez meses, Emma, con su teléfono móvil. Le extrañó que la cámara se moviera, porque no era ella quien la estaba moviendo. De repente, Heather escuchó la voz de un hombre desde el otro lado de la casa gritando: «¡Despierta, niñita, despierta!»[9].. Heather y su marido, Adam, acudieron corriendo a la habitación de Emma y, al entrar, vieron cómo la cámara del vigilabebés dejaba de enfocar a su hijita, que lloraba, y se posaba sobre Adam. La voz masculina que salía por el dispositivo que observaba a los padres pronunció una retahíla de obscenidades a la pareja adormilada, antes de que Adam recobrara plenamente la conciencia y desenchufara la cámara. El fabricante del vigilabebés, Foscam, admitió posteriormente que el dispositivo tenía una «vulnerabilidad en el *firmware*», el cual había permitido a un intruso infiltrarse sigilosamente en la cuna del bebé durmiente de los Schreck. Estos episodios distan mucho de ser aislados. Otra familia de Houston así lo descubrió cuando una voz masculina los despertó gritando el nombre de su hijita de dos años, Allyson, a la que insultaba con voz quejica: «Despierta… pequeña zorra». El intruso virtual conocía el nombre de la niña porque estaba escrito en rosa en la pared. Resulta a la vez irónico e inquietante que los dispositivos que las familias adquieren para protegerse en realidad puedan ser utilizados a modo de armas contra ellas y abrir paso a los problemas en el seno de su hogar.

Además de las cámaras vigilabebés, los sistemas de cámaras de seguridad tanto para viviendas como para las oficinas son igual de vulnerables y los investigadores han descubierto fallos generalizados en más de veinte de las marcas principales, la

mayoría de las cuales se venden con acceso remoto a Internet posibilitado mediante funciones de seguridad por omisión y débiles. Cerca del 70 por ciento de los usuarios jamás cambia el nombre de usuario por defecto, como «usuario» o «admin» ni modifican la contraseña predefinida del fabricante, como «1111» o «1234»[10]. En consecuencia, decenas de millones de cámaras conectadas a Internet quedan completamente expuestas a la interceptación por parte de desconocidos, y a los *hackers* les encanta compartir sus descubrimientos voyeristas[11]. Sin el consentimiento ni el conocimiento de las personas vigiladas, hay miles de estos canales en directo disponibles en Internet para quien quiera verlos: un Laundromat en Los Ángeles, un hombre en Newark viendo fútbol en el sofá, clientes en un bar de Virginia, una sala de estar en Hong Kong o una oficina en Moscú; para gustos, colores[12]. Habida cuenta de las oportunidades, Crimen, S. A. no tardó en explorar cuál era el mejor modo de utilizar en beneficio propio las cámaras preparadas para la Internet de las Cosas.

¿Por qué no piratear las cámaras de los bancos antes de realizar un atraco para conocer los patrones de conducta de los empleados, cuándo se realizan las entregas de dinero y las horas a las que el guardia de seguridad hace la pausa[13]? Habida cuenta que la mayoría de los atracos a bancos recaudan un botín irrisorio y comportan un alto riesgo, hay peces más gordos que pescar. Eso fue exactamente lo que dedujo una panda de delincuentes de Crimen, S. A. en marzo de 2013, cuando perpetraron un atraco a lo *Ocean's Eleven* en el Crown Casino de Melbourne, Australia[14]. Los *hackers* se apoderaron del sistema de seguridad del casino y utilizaron las cámaras de seguridad del recinto para espiar los movimientos en su interior, incluidas sus salas de juego VIP. El principal sospechoso se describió sólo como «un forastero» y era conocido por ser un «cachalote», es decir, un gran apostador. Ahora bien, esta vez jugaba con ventaja. Puesto que él y sus cómplices habían pirateado los canales de vídeo en directo, eran capaces de ver todas las cartas que tenían tanto el crupier como el resto de los jugadores en la mesa de póker. Durante sus partidas con otros grandes apostadores, los colegas *hackers* ocultos dieron al cachalote instrucciones para realizar sus apuestas a través de un auricular inalámbrico oculto. Seguro de sus bazas, el *hacker* logró ganar más de treinta y tres millones de dólares en sólo ocho manos de cartas[15]. En lugar de tentar al destino, salió de allí convertido en un hombre rico y tomó un vuelo de regreso a su propio país antes de que las autoridades tuvieran tiempo de averiguar qué había sucedido. Conforme el avance exponencial hacia la Internet de las Cosas prosiga su camino, cada vez serán más las personas que descubrirán que las cosas de confianza que esperaban que les protegieran, ya fueran cámaras de seguridad o *airbags*, pueden controlarse a distancia en su contra, de modos sorprendentes e incluso mortales.

Del robo de coches con violencia al robo de coches sin violencia

> La mayoría de personas preferiría tener un *software* malicioso en el ordenador portátil que en el interior del sistema de frenado de su vehículo.
>
> PROFESOR CHRISTOF PAAR,
> investigador de seguridad incorporada

Antes los coches funcionaban con gasolina. Hoy funcionan con código. Desde luego, sigue siendo preciso echarles gasolina o electricidad para encenderlos, pero si el código informático que incorporan no funciona, cualquier automóvil moderno está perdido. Mientras que el Chevy de 1957 de tu padre era un aparato puramente mecánico, los automóviles de hoy en día son poco más que ordenadores sobre ruedas. Cualquier coche que salga de una cadena de montaje en 2015 tendrá entre setenta y cien ordenadores a bordo, conocidos como unidades de control electrónico[16]. En conjunto, estos ordenadores gestionan el motor del automóvil, el control de la navegación, los frenos ABS, el clima, la transmisión, el entretenimiento, los limpiaparabrisas, los asientos, los seguros, la navegación, la eficiencia del combustible y el despliegue del airbag en caso necesario, por mencionar sólo algunos aspectos. Pese a que los fabricantes automovilísticos se esfuerzan porque todo quede relativamente integrado, los vehículos de hoy en día son sistemas asombrosamente complejos que contienen cerca de cien millones de líneas de código informático (frente a la cifra relativamente irrisoria de 1,7 millones de líneas de código que controlan la aviónica del cazabombardero de primera línea F-22 Raptor de las Fuerzas Aéreas estadounidenses). Todos estos circuitos electrónicos incrustados representan, de media, el 50 por ciento del coste de un nuevo vehículo (casi el 80 por ciento en el caso de los híbridos[17]). En combinación, estos microchips forman la red de zona del controlador (CAN), la red informática a bordo que es la savia de cualquier automóvil reciente y es responsable de que nuestros vehículos presenten la mejor seguridad y kilometraje y las emisiones más reducidas de toda la historia.

Estas tecnologías incorporadas no sólo se comunican entre sí internamente a través de la CAN, sino que cada vez más comparten esta información en línea con el mundo exterior a través de diversas redes de radio y móviles incorporadas en el propio automóvil. Ello aporta unas comodidades sensacionales a los conductores: la red TeleServices de BMW permite que los sensores internos del vehículo efectúen un autodiagnóstico de manera continua e informen de las averías al concesionario local. Cuando se detecta un problema, los propietarios reciben una llamada informándoles de que su vehículo tiene un problema de funcionamiento y conviene que pasen por el taller. Y el sistema OnStar de General Motors telefonea automáticamente a una ambulancia si los sensores de movimiento y *airbag* detectan que un vehículo se ha

visto involucrado en un accidente.

Si bien la cajas negras que registran datos de los acontecimientos en los vehículos pueden ayudar a los investigadores de los accidentes y reducir las primas de los seguros, también pueden «delatar» cada uno de tus movimientos, pues generan centenares de megabytes de datos por segundo[18]. Estos dispositivos rastrean de manera continua una horda de datos de vehículos, incluida tu ubicación, el uso de los cinturones de seguridad, la velocidad y el manejo de los intermitentes. Tal como admitió Jim Farley, vicepresidente mundial de *marketing* y ventas de Ford Motors, a principios de 2014, «[Sabemos] quién infringe la ley y sabemos cuándo lo hace. Hemos instalado un GPS en cada coche, así que sabemos qué hacen los conductores»[19]. Y Ford no está sola en esta empresa. El sistema OnStar de General Motors suscitó indignación cuando actualizó de manera unilateral las condiciones de servicio y se autoasignó el derecho de por vida de supervisar todos sus vehículos, incluidos los datos de localización y la lectura del cuentakilómetros, y a compartir esta información con terceras partes incluso después de que el propietario del vehículo cancelara el servicio[20]. Ah, y ese micrófono tan práctico incorporado en el coche que te permite solicitarle a OnStar indicaciones para llegar a tu destino y escuchar lo que sucede después de producirse un accidente, también puede activarse de manera remota sin tu conocimiento para escuchar a hurtadillas tus conversaciones privadas, como lleva haciendo el FBI desde 2003 en sus investigaciones relacionadas con la mafia[21].

Ahora bien, en el futuro es posible que tus preocupaciones con respecto a tu automóvil no se limiten a la privacidad. La creciente complejidad de los vehículos modernos está conduciendo a retiradas del mercado masivas debido a fallos en los sistemas y a trágicas pérdidas de vidas. Sólo en los seis primeros meses de 2014, General Motors se vio obligada a retirar veintinueve millones de vehículos, a los que se sumaron muchos otros millones de Nissan, Hyundai, Ford, Honda y BMW[22]. Cuando la electrónica profundamente compleja de un coche controla todas sus funciones principales, el hecho de que se produzcan fallos en los sistemas puede tener consecuencias imprevistas; sin ir más lejos, el aluvión de problemas que Toyota registró a finales de la primera década del siglo XXI causó la muerte a treinta y siete conductores[23]. Un jurado resolvió que muchos de los accidentes podrían haber estado provocados por deficiencias en el *software* del sistema electrónico de control del acelerador de Toyota, que hacía que el pedal continuara «pisado» y que los frenos del vehículo se inhabilitaran[24]. Se acusó a Toyota de encubrir los defectos y, en 2014, la empresa accedió a pagar una multa récord de mil doscientos millones de dólares impuesta por el Departamento de Justicia de Estados Unidos por anteponer los beneficios a la seguridad[25]. Por descontado, los temas de seguridad accidentales en los circuitos electrónicos de los vehículos son sólo parte del problema. Cuando los automóviles devienen en ordenadores, como todos los demás sistemas, se vuelven

objetivos atractivos para los *hackers* malintencionados.

La época en la que los ladrones utilizaban perchas para abrir coches está quedando relegada a la historia a marchas forzadas. Y tampoco es ya preciso apuntarle a nadie en la frente para robarle el coche; el robo de coches con violencia se ha incorporado a la edad moderna y ha sido sustituido por el robo de coches sin violencia. En Estados Unidos, todos los coches fabricados desde 1996 incorporan obligatoriamente puertos electrónicos estandarizados de diagnóstico a bordo, los cuales proporcionan acceso físico directo a los sistemas informáticos centrales de un vehículo, y una serie de protocolos de comunicaciones de la Internet de las Cosas nuevos, como RFID, Bluetooth y la telefonía móvil permiten este mismo acceso de manera remota. Los vehículos más nuevos incluso incorporan puertos USB y, como siempre, más conexiones equivale a más vulnerabilidades. De acuerdo con la Policía Metropolitana de Londres, cerca de la mitad de los ochenta y nueve mil vehículos robados en Londres en 2013 fueron manipulados electrónicamente; para ello, los delincuentes utilizaron diversos dispositivos para abrir los coches y ponerlos en funcionamiento[26]. Los artilugios que los ladrones emplean en los robos pueden adquirirse en Crimenazon.com, en su inmensa mayoría a proveedores emplazados en Bulgaria. La operación tarda menos de diez segundos en funcionar y, por supuesto, hay vídeos en Crime U que explican todo el proceso[27].

Con artilugios del tamaño de un teléfono móvil originalmente diseñados para que los cerrajeros puedan ayudar a las personas que han perdido las llaves electrónicas de sus vehículos, los ladrones se limitan a programar una nueva llave electrónica en blanco que sustituya a la original. Esta técnica de suplantación hace creer erróneamente al vehículo que la llave original del propietario está presente, llave que puede conseguirse interceptando de manera inalámbrica la señal de radio que utilizas al abrir o cerrar tu coche o atacando directamente el ordenador a bordo del vehículo.

Con sólo un ordenador portátil y un mensaje de texto SMS con las instrucciones codificadas correctas, los ladrones pueden desbloquear tus puertas, encender el vehículo y darse a la fuga[28]. Tus gustos musicales también podrían ponerte en riesgo, tal como demostraron diversos investigadores en materia de seguridad en 2011 al añadir código informático malicioso a un archivo de música MP3 y grabar una lista de canciones en un CD[29]. Cuando se reprodujo en el sistema de audio del vehículo, el archivo de canción infectado corrompió el *firmware* del vehículo y dejó una vía de acceso a los sistemas de control principales de éste para los piratas informáticos. En situaciones como ésta, el robo de un coche podría ser el mejor de todos los resultados posibles, porque una vez que los sistemas informáticos a bordo del vehículo han quedado vulnerados, las posibilidades son casi ilimitadas.

Por poco menos de treinta dólares, los *hackers* pueden montar un dispositivo de *hardware*, como una herramienta de hackeo CAN Hacking Tool, que, cuando se conecta a la red informática a bordo del vehículo, les permite hacerse con el control remoto de las luces, los cierres, el volante y los frenos[30]. Puesto que prácticamente

todos los elementos de un automóvil los gestiona un sistema informático, los dispositivos de este tipo implican que hoy es posible alargar la mano y tocar cualquier vehículo que circule por la carretera desde la otra punta del mundo subvirtiendo los receptores de telefonía móvil que incorpora. Desde una distancia más cercana, también es posible manipularlos de manera remota mediante Bluetooth y Wi-Fi. Docenas de demostraciones tanto por parte de piratas informáticos como de investigadores en materia de seguridad han elucidado que es perfectamente posible que delincuentes situados a dos mil quinientos kilómetros de distancia se hagan con el control de tu coche cuando conduces a cien kilómetros por hora por la autopista. Sólo su imaginación pone los límites a lo que hagan con tu vehículo «usurpado». ¿Poner el cuentakilómetros a cero y colocar la aguja del velocímetro en 257 km/h, incluso aunque el vehículo esté parado? Fácil. ¿Hacer sonar el claxon, poner la radio a todo trapo, apretarte el cinturón de seguridad y activar los limpiaparabrisas? Facilísimo. ¿Apagar el motor o girar bruscamente el volante hacia la izquierda para que pierdas el control del coche cuando vas a mucha velocidad? Sí, también pueden hacerlo. ¿Desplegar de repente el *airbag* y hacer que pierdas el control del vehículo y te escores cuando llevas a tus hijos en el asiento de atrás? Perfectamente posible[31]. Si un ordenador controla tu vehículo, un atacante también puede hacerlo.

El desafío que plantean estas vulnerabilidades es que no necesitan dirigirse contra un vehículo concreto, sino que, en su lugar, podrían afectar a todos los coches o vehículos de una marca, modelo y año de fabricación concretos de manera simultánea. En el caso del concesionario Texas Auto Center, un empleado corrupto fue capaz de apagar remotamente un centenar de coches. Pero empresas como OnStar han instalado su tecnología en millones de vehículos, incluida la capacidad de bloquear a distancia el encendido del motor y desactivar un vehículo en movimiento en caso de robo. ¿No podría entonces un empleado corrupto de OnStar apagar cien mil o un millón de coches? Si bien General Motors seguramente lo negaría, una vez se ha introducido una puerta negra en el coche, protegerla de que se haga un mal uso de ella deviene un duro desafío y crea la oportunidad para ataques generalizados a las infraestructuras tanto por parte de *hackers* como de Estados nación.

A medida que las redes de sensores ambientales proliferen y la tecnología de los vehículos mejore, los seres humanos cederán cada vez más el control de su responsabilidad como conductores a las máquinas. El director ejecutivo de Renault Nissan, Carlos Ghosn, ha anunciado que su empresa contará con un vehículo autoconducido completamente autónomo disponible en el mercado general en 2020, y el plan de Volvo es poner a disposición del público vehículos de este tipo en 2017[32]. El mayor partidario de estas tecnologías ha sido Google, cuyos propios vehículos autoconducidos en pruebas han recorrido más de un millón de kilómetros sin sufrir ni un solo choque o accidente[33]. Se trata de un aspecto relevante, porque resulta que los seres humanos somos unos conductores pésimos y más de treinta y tres mil estadounidenses mueren en accidentes de tráfico cada año. Una red de vehículos

autónomos completamente automatizada que funcionara bien podría evitar miles de muertes innecesarias y ahorrar miles de millones en costes económicos derivados. A medida que el precio de estas tecnologías descienda, podríamos ver cómo los conductores de UPS y los taxistas son sustituidos por alternativas autónomas y más baratas, que además no se afilian a sindicatos.

Con todo, los vehículos de hoy en día, ya los conduzcan personas, una inteligencia artificial, datos masivos o redes de sensores, siguen siendo ordenadores con ruedas, accionados por sistemas de datos inseguros que se comunican a través de protocolos de transmisión completamente pirateables. Como tales, el futuro podría no ser tan halagüeño como sugieren los defensores de los vehículos autónomos. Cuando la mayoría de los vehículos se una a la Internet de las Cosas, no pasará demasiado tiempo antes de que algún atacante deshonesto se haga con el control de un coche y lo convierta en un arma de varias toneladas de peso de metal, vidrio y combustible explosivo. De la misma manera que tanto Crimen, S. A. como las exparejas enloquecidas atacan ordenadores y teléfonos móviles, cabe esperar que en el futuro también dirijan sus embestidas contra coches y acerquen a la realidad escenas como las del *thriller* de terror que Stephen King escribió en 1983 acerca de un coche poseído llamado Christine. Los cuerpos de seguridad son plenamente conscientes de esta amenaza y, en julio de 2014, el FBI advertía en un informe interno que los vehículos sin conductor podían ser utilizados como «armas letales, pues los terroristas podían introducir en ellos explosivos y programarlos para que se dirigieran a un destino concreto»[34]. Los vehículos autónomos también podrían detenerse de golpe y paralizar por completo el tráfico en una ciudad o país.

Para ser sinceros, algunos de estos ataques vehiculares requieren unos conocimientos informáticos muy avanzados para llegar a buen puerto, pero, tal como hemos visto en el caso de otras vulnerabilidades, no tardará en haber opciones de *crimeware* «de apuntar y hacer clic» también para el robo de coches sin violencia. Los fabricantes automovilísticos están empezando a tomar nota, sobre todo ahora que se publican listas con «los coches más fáciles de piratear». Del mismo modo que en el pasado los vehículos se categorizaban por su seguridad en caso de accidente, hoy en día los investigadores en materia de seguridad determinan qué coches son más fáciles de vulnerar (y la respuesta es: Jeep Cherokee, Cadillac Escalade, Infiniti Q50 y Toyota Prius[35]). En un guiño a esta inquietud creciente, Tesla, empresa creadora de algunos de los vehículos tecnológicamente más avanzados en las carreteras de hoy en día, contrató a un gurú en materia de seguridad de alto nivel de Apple para cubrir este aspecto[36]. Ahora bien ¿qué nuevas amenazas permitirán estas tecnologías en el futuro cuando Crimen, S. A. se haga remotamente con el control de tu coche autónomo, bloquee las puertas, pise a fondo el acelerador y te conduzca a un almacén abandonado en una zona insegura de la ciudad? Pese a que podrías intentar en vano escapar, lo último que los testigos asegurarían sería haberte visto gritando de terror y golpeando con los puños las lunas del vehículo desde dentro, incapaz de reaccionar a

la siguiente generación de secuestro. Por supuesto, asumiendo que regresaras vivo a casa en tu vehículo potencialmente poseído por un pirata informático, podrías encontrar otros problemas a la espera, si en tu ausencia tu hogar también se ha unido a la Internet de las Cosas.

Hogar, pirateado hogar

Desde los días de *Los Supersónicos* nos han prometido un hogar de la era espacial repleto de aparatos robóticos y extravagantes artilugios electrónicos destinados a garantizarnos una buena vida con sólo accionar un botón. Y pese a que aún no vamos en autos voladores, estos dibujitos animados de Hanna-Barbera de principios de la década de 1960 fueron proféticos al predecir la existencia de televisores de pantalla plana, chats de vídeo y puertas correderas automáticas. En teoría, el hogar en red moderno suena fantásticamente bien. Sistemas de seguridad y videocámaras nos protegerán de los ladrones y contactarán con la policía si alguien rompe una ventana. Y los termostatos digitales interactuarán con las previsiones climáticas de las coordenadas de GPS específicas de tu vivienda y ajustarán de manera inteligente la calefacción y el aire acondicionado para garantizar una eficiencia, una comodidad y un ahorro máximos. Los sensores inteligentes en el sótano detectarán si hay agua en el suelo en caso de reventar una tubería y cortarán de manera automática el paso del agua por la zona afectada. Tu teléfono móvil cerrará la puerta de tu casa a través de Internet para que no tengas que volver a preocuparte cuando, de camino hacia el aeropuerto, te asalte la duda de si has echado la llave o no. Los frigoríficos inteligentes nos avisarán cuando la leche esté a punto de caducar y, ante el mero acto de tirar una caja de cereales vacía al cubo de la basura, se utilizarán tus datos de la tarjeta de crédito guardados para encargar más cereales sin que tengas que mover ni un dedo. Pero ¿realmente te interesa que el cubo de la basura tenga el número de tu tarjeta de crédito?

Se espera que el mercado de la domótica en Estados Unidos «alcance los 16 400 millones en torno a 2019», y todas las grandes empresas de tecnología compiten por llevarse un pedazo del pastel[37]. Es posible que ya haya elementos de tu hogar unidos a la Internet de las Cosas, dado el número creciente de utilidades que instalan medidores inteligentes para calcular y regular el consumo de agua, electricidad y gas. Sin embargo, quizá algunas de las mayores oportunidades se presenten en el espacio de los productos de consumo, donde Google, Apple, Samsung y Microsoft, por nombrar sólo a unas cuantas empresas, compiten por convertirse en el nexo central y el sistema operativo de tu hogar para permitirte supervisar y manipular desde la distancia tu humilde morada utilizando el pasaporte automático a tu vivienda mientras estás de camino.

Apple reveló recientemente su HomeKit, incluido con el iOS 8, que lleva el gusto por el diseño del gigante de Cupertino a la domótica, al permitir a los usuarios cerrar sus puertas, atenuar las luces y reproducir sus equipos estéreo con sólo tocar sus iPhone o solicitándoselo en voz alta al agente de inteligencia artificial de la empresa, Siri. La simple mención de las palabras «ir a dormir» hará que HomeKit realice de manera automática una serie de acciones, como cerrar las cortinas, bajar la temperatura y apagar las luces, si bien, dada la experiencia que algunos han tenido con el reconocimiento de voz de Siri, podrían provocarse situaciones hilarantes si, por ejemplo, la televisión se pone en marcha de repente o se enciende el coche y se abre la cerradura de la puerta de tu casa. De todos modos, con el tiempo estos problemillas se resolverán y los nexos digitales centralizados en nuestro hogares gestionados por nuestros teléfonos móviles se convertirán en una realidad en el futuro próximo. ¿Qué podría entonces salir mal?

Pues, para empezar, hasta ahora nunca habías tenido que actualizar el *firmware* de la lavadora, ni que reinstalar el sistema operativo de tu hogar y reiniciarlo para que la puerta de entrada funcionara. Si bien conectar bombillas, tostadoras, lavadoras, televisores, cierres de puertas, sistemas de seguridad, cámaras vigilabebés, termostatos, lavabos, farolas y bañeras a la Internet de las Cosas podría ofrecer una comodidad propia de *Los Supersónicos*, la incorporación de todos estos objetos a la Internet de las Cosas por supuesto comportará sus propios riesgos en materia de privacidad y seguridad. Muchos de estos sistemas no utilizan ningún protocolo de autenticación o encriptación para establecer comunicaciones entre un electrodoméstico, un dispositivo móvil y un sistema domótico[38]. Por tanto, es posible burlarlos, piratearlos, interceptarlos y subvertirlos fácilmente. Un estudio realizado por HP en julio de 2014 detectó que el 70 por ciento de los dispositivos conectados a la Internet de las Cosas eran vulnerables a ataques y cada objeto contenía de promedio veinticinco fallos de seguridad únicos[39].

Una vez tu vivienda esté totalmente conectada en línea, no hay motivo para pensar que los *hackers* no la consideren un objetivo viable, y todas las evidencias sugieren que ya se han puesto manos a la obra. Cada atacante tendrá su propia motivación: el crío de los vecinos al que le espetaste que no pisara el césped, el exnovio con un ataque de celos, el mirón con quien una vez te cruzaste en la frutería o un gobierno foráneo decidido a explotar las posibilidades del ciberespionaje. Para Crimen, S. A., en cambio, lo importante siempre será el dinero y aprovechará las debilidades de los dispositivos de Internet de las Cosas de tu hogar para acceder a datos valiosos almacenados en tu red o para perpetrar robos cotidianos. Ah, ¿y recuerdas el CryptoLocker, el *ransomware* que se hace con el control de los ordenadores portátiles y móviles y los bloquea encriptándolos? Pues ya puedes esperar que en la clandestinidad digital se vendan kits de herramientas de *crimeware* para dejarte encerrado en tu casa o incapaz de acceder a ella y te veas obligado a pagar un rescate en bitcoins para que tu hogar vuelva a abrirse y a funcionar.

Tus hijos pueden afrontar amenazas similares cuando «juegan a mamás y papás». Los grandes fabricantes de juguetes, como Disney y Mattel, ya están estudiando la Internet de las Cosas, y ya existen un montón de muñecas, peluches y robots en miniatura con Wi-Fi abriéndose paso hacia ti en esta «Internet de los Juguetes»[40]. Pero los juguetes también pueden subvertirse y, al menos uno de ellos, el conejito interactivo de plástico Karotz, que puede controlarse mediante una aplicación para teléfono móvil e incluye una cámara, un micrófono y un chip RFID, ya se ha manipulado, cosa que permitiría a un acosador vigilar a tu hijo con una cámara de vídeo[41].

Otras tecnologías, incluida la bombilla de 135 años de antigüedad, están siendo reinventadas para ajustarse a la Internet de las Cosas, y sistemas como el de iluminación por LED Philips Hue permiten a los consumidores apagar o encender las luces mediante sus teléfonos móviles. Pero también permiten que las apaguen los *hackers*, gracias a un fallo conocido en la seguridad del sistema Philips, lo cual puede resultar alarmante dado el vínculo evidente entre la iluminación y la seguridad física[42]. Otros sistemas, como la bombilla inteligente y energéticamente eficiente LIFX, filtran la contraseña del router Wi-Fi de tu hogar una vez se conectan a una lámpara y lo dejan expuesto ante cualquier *hacker* que se ponga en contacto con «la bombilla maestra» de la red de tu hogar[43]. Las lámparas y bombillas también pueden tener puertas traseras incorporadas, similares a las de aquellas planchas chinas descubiertas en Rusia. A principios de 2014, unos *hackers* crearon una lámpara-espía capaz de tuitear en directo tus conversaciones privadas. El dispositivo, conocido como Conversnitch, cuesta menos de cien dólares y parece una bombilla estándar; la única diferencia es que lleva oculto un micrófono que escucha todas las conversaciones que tienen lugar a su alrededor[44]. Para demostrarlo, los creadores del dispositivo grabaron un vídeo en el que ellos mismos colocaban sin problemas dispositivos Conversnitch en bibliotecas, oficinas, restaurantes McDonald y una sucursal bancaria, todo ello sin ninguna interferencia ni llamada de atención por parte del personal de estos lugares, lo cual presagia una nueva y potente herramienta de la Internet de las Cosas destinadas al espionaje industrial.

A medida que los dispositivos inteligentes proliferen, estarán controlados por sistemas domóticos centralizados, la mayoría de los cuales ya se han vulnerado en algún momento, lo cual permitirá a los piratas informáticos hacerse con el control de todos los dispositivos conectados a tu red local. Será como *Pesadilla en la calle de la Domótica*. Pese a que seguramente dormiremos mejor creyendo que estamos sanos y salvos en nuestras viviendas con IoT, la invasión doméstica 2.0 es mucho más sencilla de lo que piensas, tal como demostró la periodista de *Forbes* Kashmir Hill. Mientras trabajaba en un reportaje sobre la Internet de las Cosas, Hill se limitó a buscar en Google el término «hogares inteligentes» y de inmediato localizó a ocho familias que utilizaban el popular sistema domótico Insteon, que controla electrodomésticos como «bombillas, bañeras, ventiladores, televisores y puertas de

garaje».

Puesto que Insteon no requería introducir nombre de usuario ni contraseña y permitía que sus productos fueran rastreables por los motores de búsqueda, la periodista de *Forbes* fue capaz de localizarlos sin dificultad (sí, ahora alguien puede buscar en Google tu frigorífico inteligente y comunicarse con él a distancia[45]). A continuación, Hill contactó con los inocentes implicados, se presentó y les comentó: «Puedo ver todos los dispositivos de su hogar y creo que puedo controlarlos». Les pidió permiso para probarlo y los asustados dueños de las viviendas situadas a miles de kilómetros de distancia accedieron a regañadientes mientras la periodista tomaba fácilmente el control de sus dispositivos. El Insteon Hub no fue el único[46]. Un estudio realizado en 2013 reveló que los *hackers* eran capaces de infiltrarse fácilmente en el 80 por ciento de los hubs de hogares domóticos más habituales, incluido VeraLite Controller, compatible con más de 750 productos domóticos.

La cantidad de vulnerabilidades en los sistemas domóticos es tan elevada que, en 2014, el Computer Emergency Readiness Team del Departamento de Seguridad Nacional de Estados Unidos se vio obligado a emitir una alerta pública a los quinientos mil usuarios del popular dispositivo domótico WeMo de Belkin en la que identificaba cinco puntos débiles distintos del producto[47]. La advertencia destacaba que «un intruso remoto no autenticado podría introducir *firmware* malicioso, transmitir conexiones dañinas o acceder a archivos del sistema del dispositivo para hacerse con el control absoluto de éste». El Departamento de Seguridad Nacional de Estados Unidos añadía: «Actualmente no conocemos ninguna solución práctica para este problema». Un artículo sobre este incidente destacaba que «una vez un atacante ha establecido una conexión con un dispositivo WeMo que forme parte de la red de la víctima, dicho dispositivo puede utilizarse como punto de apoyo para atacar otros dispositivos, como ordenadores portátiles, teléfonos móviles y el almacenamiento de archivos en red adjunto». Esta última advertencia reviste importancia. Los piratas informáticos no intentarán colarse en el dispositivo más seguro de tu red, como puede ser un ordenador portátil encriptado y apagado que utilice un programa cortafuegos. En su lugar, siempre atacarán el eslabón más débil, la cafetera WeMo con Internet que forma parte de tu red doméstica, precisamente la que carece de protocolos de seguridad o cuenta con unos inadecuados. Una vez se hayan infiltrado en la cafetera, habrán roto el perímetro de la línea Maginot virtual de tu red y, desde allí, les bastará dar un saltito para infectar y atacar los dispositivos más seguros y rentables de tu hogar.

Uno de los objetos online más habituales en muchos hogares y empresas es el sistema de alarmas de seguridad, en el que más de treinta y seis millones de estadounidenses confían para velar por la seguridad de sus familias. Sin embargo, ya sea a través de sus sencillos sensores en la puerta o en los teclados, también son fáciles de piratear, tal como hemos visto en todas esas películas de Hollywood al estilo de *Misión: Imposible*. La mayoría de los sistemas de alarma, incluidos los de

empresas como ADT y Vivint, utilizaban protocolos de comunicaciones inalámbricas tradicionales de la década de 1990 que no servían para encriptar o autenticar sus señales de transmisión. En consecuencia, las mismas cámaras que supuestamente deben proteger pueden volverse contra sus propietarios para espiar sus actividades y sus alarmas pueden desactivarse para que no suenen cuando un intruso se cuele en sus hogares[48].

Pero no sólo los sistemas de alarma antiguos son vulnerables; protocolos de radiocomunicaciones de la Internet de las Cosas más nuevos como Z-Wave también pueden piratearse, lo cual resulta desconcertante, dado que hay ciento sesenta fabricantes que los utilizan, se emplean en miles de empresas, como el hotel Wynn de Las Vegas, que ha instalado sesenta y cinco mil dispositivos Z-Wave en sus habitaciones[49]. También la cadena hotelera Hilton anunció que permitiría a sus huéspedes utilizar sus teléfonos inteligentes como llave para abrir las puertas en cuatro mil hoteles de todo el mundo hacia finales de 2014[50]. A medida que más y más puertas principales y cerrojos pasen a estar online, es posible que abran las puertas a la invasión doméstica 2.0. Los cacos podrán piratear tu puerta principal desde sus teléfonos inteligentes y desactivar tus alarmas, lo cual les garantizará que en estos hogares nadie te escuchará gritar.

Ahora bien, no sólo es posible dirigir ataques contra hubs domóticos centralizados, sino también contra dispositivos «inteligentes» individuales, como televisores. De hecho, numerosos informes indican que mientras estás apoltronado mirando tu televisor inteligente, es posible que él también te esté mirando a ti. La mayoría de los televisores de gama media o alta existentes en la actualidad son compatibles con la Internet de las Cosas y se suministran de fábrica con aplicaciones instaladas, como Netflix, Skype, Facebook y Hulu, aparte, claro está, de las cámaras, micrófonos y puertos USB que incorporan. En 2013 las ventas mundiales de televisores inteligentes alcanzaron cerca de noventa millones y dentro de poco costará encontrar televisores «tontos» tradicionales, una tendencia potencialmente alarmante para aquéllos que valoran la privacidad y la seguridad[51]. Se ha detectado que muchas marcas presentan vulnerabilidades en cuestión de seguridad, como los televisores Samsung Smart, que permitían a los *hackers* activar a distancia la cámara remota pensada para realizar llamadas a través de Skype y tomar de manera subrepticia fotografías instantáneas de los espectadores y observarlos en sus salas de estar y dormitorios[52].

Los *hackers* también lograron robar las credenciales de inicio de sesión y los datos de la cuenta almacenados en las aplicaciones inteligentes de los televisores Samsung para hacerse con el control de las cuentas del usuario en Facebook y otras redes sociales. Y a aquellos consumidores confiados que además habían utilizado el puerto USB del televisor para conectar un disco duro y poder reproducir en *streaming* música y vídeo en directo en sus televisores les aguardaba aún otra sorpresa desagradable. Los *hackers* podían ver, descargarse y borrar esos archivos a través del

televisor: malas noticias para quienes guardaban detalles financieros o documentos personales en sus discos duros externos. Estas conexiones adicionales en el hogar exponen a los usuarios a un ataque similar al sufrido por Mat Honan, quien perdió valiosas fotografías y otros datos almacenados localmente porque alguien con malas intenciones los borró de manera remota.

Crimen, S. A., como Silicon Valley, está poniendo a prueba los mejores métodos para monetizar la Internet de las Cosas y, como parte de este proceso, ha actualizado sus tácticas de eficacia demostrada para la era de la informática ambiental. A principios de 2014, unos *hackers* se hicieron con el control de más de cien mil objetos «inteligentes» cotidianos, incluidos entre ellos encaminadores domésticos, alarmas antirrobo, *webcams*, cajas multimedia y frigoríficos, y los unieron para crear el primer *botnet* de electrodomésticos del hogar de la historia. Los atacantes utilizaron los dispositivos para enviar más de «750 000 mensajes de correo electrónico de *phishing* y *spam* malicioso», cada uno de ellos destinado a reportar beneficios a Crimen, S. A.[53] Que un frigorífico reciba mensajes de correo no deseado desconcierta, si bien conviene recordar que los dispositivos inteligentes son ordenadores completos y, una vez se vulneran, pueden utilizarse como cualquier otro ordenador de sobremesa pirateado, tanto para albergar pornografía infantil como para sobrecargar sitios web concretos con volúmenes descomunales de datos inútiles[54]. Reunir un millón de ordenadores actuales para formar un ejército de *botnets* ya es suficientemente malo, pero la incorporación de otros cincuenta mil millones de objetos inteligentes a la Red, todos ellos con una seguridad nula o escasa, brindará magníficas oportunidades para perpetrar ataques informáticos ofensivos.

Los *botnets* aumentarán de tamaño y pasarán de estar integrados por millones de máquinas vulneradas a estar formados por, potencialmente, miles de millones, cosa que traerá con ellos nuevas formas de WMD (armas de alteración masiva). Empleando estas ciberarmas, Crimen, S. A. contará con potentes herramientas nuevas en su arsenal para extorsionar a empresas e individuos por igual, a quienes mantendrá desconectados hasta que le abonen «un impuesto revolucionario» en bitcoins. La potencia informática incorporada en los objetos inteligentes diseminados por tu hogar y oficina puede resultar muy provechosa para los delincuentes de muchos otros modos adicionales. A principios de 2014, los investigadores descubrieron que decenas de miles de grabadores de vídeo digital con Internet habían sido vulnerados con el gusano Linux.Darlloz con la finalidad de utilizar su poder de procesamiento para extraer criptodivisas como MinCoins y Dogecoins[55]. De este modo, los piratas pueden hacer que tus dispositivos funcionen a plena velocidad y generar monedas virtuales para ellos mientras te cargan a ti la factura eléctrica por utilizar tus electrodomésticos las veinticuatro horas de los siete días de la semana. En teoría, el nuevo contador inteligente que hay instalado en tu hogar podría detectar un uso abusivo de la electricidad, pero también es posible vulnerarlo.

Lo que sabe el enchufe

Los contadores inteligentes serán un elemento nuclear de la Internet de las Cosas global y sus capacidades de comunicación bidireccional permitirán registrar y llevar un seguimiento de los detalles del uso de la electricidad tanto en hogares como en empresas con el fin de mejorar la eficiencia general y la fiabilidad de un tendido eléctrico desfasado y sobrecargado. A mediados de 2013 se habían instalado contadores inteligentes en más de cuarenta y seis millones de hogares estadounidenses, y el Reino Unido prevé su despliegue en toda Gran Bretaña antes de 2020[56]. La información de los contadores inteligentes, gran parte de la cual se transmite sin encriptar, puede revelar detalles como la marca y la antigüedad de tus electrodomésticos, cuándo los utilizas y en qué estancias de tu hogar. La extrapolación de estos datos permite averiguar cuánto tiempo pasas cocinando y cuándo enciendes la televisión en el dormitorio. Sin embargo, el elevado nivel de detalle que los contadores inteligentes pueden proporcionar con respecto a tus actividades va mucho más allá de saber simplemente que utilizaste el microondas a las 19:26 el jueves.

Investigaciones realizadas en Alemania revelaron que los contadores inteligentes también podían informar de qué programas televisivos veía el público y a qué horas, debido a la electricidad específica requerida para mostrar las escenas de cada programa en la pantalla[57]. Midiendo estos datos en conjunto, el equipo de investigación fue capaz de crear perfiles individuales para todos los programas televisivos y resulta que el episodio 71 de *Star Trek* tiene una firma eléctrica distinta de la del episodio 17 de *Modern Family*. Es evidente que pueden generarse muchos millones de dólares vendiendo esta información a terceras partes. De hecho, en mayo de 2014, WPP, la mayor agencia de publicidad del mundo, anunció que formaba equipo con la empresa de análisis de datos londinense Onzo con vistas a estudiar modos de recopilar los datos de los contadores inteligentes para, finalmente, «abrir la puerta de casa» a los anunciantes.

Las amenazas procedentes de los contadores inteligentes van mucho más allá de las profundas implicaciones en temas de privacidad, y ya se han producido ataques contra dispositivos inteligentes no seguros con multitud de finalidades, pero sobre todo para cometer fraudes financieros. En Puerto Rico, por ejemplo, Crimen, S. A. empleó grandes equipos de tecnomafiosos para aprovechar la instalación generalizada de contadores inteligentes en la isla. Empleando *software* ampliamente disponible en la clandestinidad digital y un sencillo ordenador portátil, los *hackers* malhechores empezaron a realizar «llamadas de servicio» tanto a empresas como al público general. Por unos precios que oscilaban entre los 300 y los 1000 dólares para las viviendas y 3000 para los comercios, Crimen, S. A. reprogramó con éxito los contadores inteligentes con el fin de ahorrar a sus «clientes» hasta el 75 por ciento de

sus facturas de electricidad mensuales. Según una investigación de aquel incidente llevada a cabo por el FBI, la autoridad de energía y electricidad puertorriqueña afectada perdió cerca de cuatrocientos millones de dólares en ingresos anuales[58]. Como todos los ordenadores, los contadores inteligentes también son vulnerables a ataques de *software* malicioso y los investigadores en materia de seguridad de IOActive crearon un gusano capaz de propagarse velozmente de un contador inteligente infectado en un hogar a otro, hasta acabar infectando a todo un vecindario y sumirlo en la oscuridad[59].

El termostato inteligente de la pared de tu vivienda trabajará codo con codo con el contador inteligente. De hecho, hay una empresa que está superando con creces a la competencia y revolucionando el mercado: Nest Labs. Fundada por dos antiguos ejecutivos de Apple, Nest ha reinventado por completo el tosco termostato del pasado, que no había cambiado demasiado desde la década de 1950. Aprovechando la profunda experiencia en diseño obtenida en Apple, los fundadores de Nest crearon un bello termostato por Wi-Fi repleto de sensores de última generación, incluidos sensores de temperatura, de detección de movimiento, de humedad y de luz. Nest emplea algoritmos de inteligencia artificial adaptativos diseñados para aprender qué temperaturas te gustan más y cuándo. Además, incorpora un modo de ausencia automático que determina cuándo no ha habido ningún movimiento ni se ha encendido ninguna luz cerca del dispositivo y deduce correctamente si estás de vacaciones o no estás en casa. Los termostatos Nest se han convertido en una opción sumamente popular entre el público general y cada mes se vende un centenar de miles de unidades, junto con otros productos de la marca, como su alarma antiincendios con Wi-Fi multisensor y parlante[60]. El entusiasmo generalizado que ha suscitado no ha pasado desapercibido a otros gigantes de la tecnología y, en 2014, pocos años después de su creación, Nest fue adquirida por Google por 3200 millones de dólares, lo cual fue una buena notica para los fundadores de Nest y su centenar aproximado de empleados, pero ¿por qué iba a querer una empresa de publicidad en Internet adquirir un fabricante de dispositivos IoT?

Google conoce bien las oportunidades que brinda la Internet de las Cosas, y Nest es un potente producto de *hardware* para anclar sus ambiciones en la batalla de lo que se está denominando «el hogar consciente»[61]. No obstante, los termostatos y los detectores de humo Nest, dotados de multitud de sensores, son productores de datos prodigiosos y, del mismo modo que los teléfonos móviles Android generaron nuevas oportunidades de ventas de datos y publicitarias, también lo harán los productos de Nest Labs. Es más, Google no ha acabado con sus adquisiciones, ni mucho menos. En junio de 2014 anunció la compra de Dropcam, una empresa novel de seguridad mediante videocámaras de grandes dimensiones, por 555 millones de dólares. Dropcam fabrica cámaras de seguridad de alta definición dotadas de Wi-Fi y Bluetooth que reproducen en directo vídeo en aplicaciones móviles y envían alertas basadas en actividades predeterminadas que los dispositivos notan. Con la compra de

Dropcam, Google no sólo posee hoy tus búsquedas en la Red, tu correo electrónico, tu teléfono móvil, mapas y localización, sino que también conoce los movimientos que realizas en el interior de tu hogar gracias a los canales de retransmisión de vídeo en directo. De ahí que tanto tu termostato como el detector de incendios y el sistema de seguridad vayan acompañados de largas condiciones de servicio. ¿Podrían ser más evidentes las implicaciones para la seguridad?

Por descontado, un contador inteligente inseguro y accesible es un modo fantástico de saber cuándo uno se ausenta de casa durante largos períodos de tiempo. En lugar de buscar tus publicaciones en Facebook, a los cacos del mañana les bastará con echar un vistazo a tus canales de vídeo en directo, solicitar a tu frigorífico cuándo fue la última vez que se abrió su puerta o simplemente preguntar al termostato inteligente si se encuentra en modo de vacaciones prolongado. El termostato Nest de Google ya se ha vulnerado con éxito y ha permitido justo eso: ofrecer a los *hackers* un acceso remoto potencial al dispositivo e incluso monitorizar si el inquilino de una casa está o no en su hogar mediante el detector de movimiento incorporado o incluso poner la calefacción a toda potencia[62]. Otro de los productos estrella de Nest, el detector de humos y monóxido de carbono Nest Protect, también ha experimentado dificultades, y 440 000 dispositivos tuvieron que ser retirados del mercado debido a un fallo del *software* que podía retrasar la activación de la alarma en caso de incendio[63]. Las cámaras Dropcam también presentan vulnerabilidades en materia de seguridad, que los *hackers* pueden aprovechar para ver vídeos remotamente, activar el micrófono de la cámara e inyectar vídeo falso en el canal de vídeo en directo online del dispositivo, en el caso de que los ladrones quieran actuar como en *Ocean's Eleven*, sin dejar rastro[64]. Huelga decir que a Crimen, S. A. también le interesa saber lo que saben tus enchufes: tal vez descubras que con cada nueva bombilla o cerradura Wi-Fi que adquieras, estarás proporcionando a los *hackers* sin saberlo todo lo que necesitan para encontrar nuevos modos de acechar tu hogar desde la distancia.

Ataques a empresas y a edificios

Las empresas también se están apuntando a la moda de la Internet de las Cosas con el fin de recortar sus costes y, aunque la mayoría de ellas cuentan con jefes de seguridad informática, el campo de batalla tecnológico que supone una oficina está demostrando ser extremadamente difícil de gestionar. Prácticamente nadie sabe que, desde 2002, casi todas las fotocopiadoras incorporan discos duros internos que guardan todos los documentos copiados o escaneados con ellas. Puesto que muchos de estos dispositivos se alquilan o acaban vendiéndose, los datos que contienen quedan expuestos a posibles robos, tal como demostró un reportaje de investigación

de la CBS News. En un almacén de Nueva Jersey se encontraron seis mil fotocopiadoras usadas al a venta, todas ellas cargadas con secretos empresariales y gubernamentales penetrantes. El equipo periodístico de investigación adquirió cuatro de aquellas fotocopiadoras usadas para comprobar qué podía recuperar, y los resultados fueron escandalosos. Empleando herramientas de recuperación de datos sencillas y ampliamente disponibles, los investigadores encontraron «decenas de miles de documentos», incluidas «noventa y cinco páginas de nóminas, con nombres, direcciones postales y números de la seguridad social», «copias de cheques por valor de 40 000 dólares», «trescientas páginas de historiales médicos individuales» del Affinity Health Plan, que incluían todo, desde recetas de medicamentos hasta diagnósticos de cáncer, «denuncias de violencia doméstica detalladas y una lista de violadores buscados» de la Unidad de Delitos Sexuales del Departamento de Policía de Buffalo y una «lista de objetivos en una importante redada antidrogas» de su brigada de narcóticos[65].

Huelga decir que en el mundo conectado en red de la Internet de las Cosas, no hace falta ni siquiera tener acceso físico a las fotocopiadoras, pues todos esos documentos pueden extraerse de ellas de manera remota. Los *hackers* acceden a las fotocopiadoras en red (la inmensa mayoría de las cuales están conectadas a Internet en cualquier oficina moderna) desde hace tiempo y han estado observando qué se fotocopiaba en tiempo real[66]. Más aún, las impresoras de oficina, como la HP LaserJet Pro, se han pirateado a distancia para obtener acceso sin autorización a redes Wi-Fi y a sus contraseñas de administrador, que el dispositivo guarda en texto simple sin encriptar[67]. Un ataque al *firmware* incrustado descubierto en 2011 demostró que millones de impresoras HP podían recibir remotamente instrucciones de actualización que enviaban *hackers* y hacían que los dispositivos funcionaran a toda velocidad, por lo que acababan incendiándose. Aprovechando una vulnerabilidad del fusor de la máquina, los *hackers* conseguían que la impresora se sobrecalentara, quemara el papel que pasaba por dentro de ella y, al final, estallara en llamas[68]. Gracias a la Internet de las Cosas, ahora es posible provocar un incendio desde miles de kilómetros de distancia, y yo no contaría con el detector de incendios conectado a la IoT para que me salvara, porque cualquier *hacker* lo bastante motivado como para incendiar tu oficina u hogar, seguramente también habrá desactivado todos los sistemas de seguridad para detectar humo.

Asimismo, es posible manipular otro material de oficina habitual, incluido el equipo para videoconferencias que suele encontrarse en la mayoría de las oficinas y salas de juntas, donde se debaten algunos de los secretos corporativos guardados con más celo. Tal como las cámaras de tu vivienda pueden permitir a un *hacker* contemplar tus actividades a vista de pájaro, estos ojos digitales también funcionan en el lugar de trabajo. Los sistemas de videoconferencias, como los de Polycom y Cisco, de uso extendido en las oficinas modernas, han demostrado ser fácilmente vulnerables a ataques. Para demostrarlo, un *hacker* programó un *script* que detectara

todos los sistemas de videoconferencias inseguros a su alcance y, al poco, había descubierto más de «cinco mil en salas de conferencias en despachos de abogados, empresas farmacéuticas, refinerías de petróleo y centros médicos»[69]. Entre los canales de vídeo en directo a los que pudo acceder figuraban una reunión entre un abogado carcelario y un preso, «una sala de operaciones en un centro médico universitario, una oferta de capital riesgo donde las cuentas confidenciales de la empresa se proyectaban en una pantalla» e incluso la sala de juntas de Goldman Sachs. Este experimento demuestra que incluso en la oficina, cuando todo está conectado, todo es vulnerable. Puesto que muchos de los sistemas Polycom y otros sistemas de videoconferencias se venden, instalan y mantienen sin protocolos de seguridad serios activados y con la respuesta automática activada por admisión, los *hackers* pueden llamar desde la distancia y encender las cámaras y los altavoces para espiarte a ti y a tu empresa.

Entre tanto, en todo el mundo, equipos de construcción se dedican a crear nuevos edificios «inteligentes», tanto rascacielos como almacenes y fábricas, y adecúan los que ya existen. Conectar un edificio a Internet ofrece unos ahorros potenciales nada desdeñables para los propietarios de la propiedad, que pueden aprovechar complejos sistemas automatizados para ahorrar en costes de agua, electricidad y gas en edificios que perciben nuestra presencia y aprenden a desconectarse según convenga cuando la gente entra y sale de ellos. Hoy en día, todos los sistemas de calefacción, ventilación y aire acondicionado (HVAC) se ponen online e integran diversas alamas, sensores, lectores de tarjetas de seguridad, cámaras e incluso objetos físicos, como máquinas expendedoras, tuberías de agua, vallas de *parking* y ascensores, todos ellos controlados centralmente mediante sistemas operativos de gestión de edificios. Hay pruebas de estas «mejoras» por doquier y, en multitud de grandes edificios de oficinas, como los de Manhattan, los ascensores no tienen botones numerados de manera individual para que selecciones la planta a la que te diriges. En su lugar, los datos codificados en tu placa RFID o los controles de una estación de seguridad central predeterminan a qué plantas te llevará el ascensor.

Al igual que sucede con tu hub domótico, los sistemas de gestión de edificios comerciales también pueden piratearse y, cuando esto ocurre, los resultados pueden ser sorprendentes. En abril de 2012, alumnos del MIT accedieron ilegalmente al Green Building, el edificio de veintiuna plantas que alberga el Departamento de Ciencias de la Tierra, Atmosféricas y Planetarias de la universidad, y emplearon los sistemas eléctricos vulnerados para crear un inmenso juego *Tetris* multicolor al cual podía jugarse de verdad[70]. Una consola de videojuegos inalámbrica conectada al edificio permitía a los «jugadores» mover, girar y dejar caer bloques, que correspondían a las luces de diversas oficinas. Desde el otro lado de la calle y en todo Cambridge se veía cómo las luces de las ventanas de las oficinas del edificio se encendían y desplazaban como si los *hackers* estuvieran jugando al famoso videojuego de puzle ruso. Y pese a que algunas infiltraciones ilegales en edificios

pueden ser divertidas, otras tienen costes mucho mayores.

Los sistemas que por tradición habían funcionado como entidades autónomas se están unificando en la actualidad y las interconexiones de amplio alcance de la Internet de las Cosas pueden demostrar ser sumamente difíciles de anticipar, mapear y proteger. Para lidiar con estos desafíos, muchas organizaciones están recurriendo a la gestión centralizada de los sistemas de sus edificios y, por ejemplo, subcontratan a una empresa externa especializada en seguridad para que supervise de manera remota todos los canales de seguridad de una empresa concreta en numerosos sitios. Cuando todo está conectado, otros servicios, incluidos los sistemas de climatización, también pueden controlarse centralmente, y una empresa que lo hace es Target, que ha externalizado sus responsabilidades de calefacción y refrigeración a un comerciante conocido como Fazio Mechanical Services de Pensilvania. Desde sus oficinas centrales, los técnicos de Fazio se comunican directamente con el sistema de gestión de servicios y suministros contratados de Target, un filón que Crimen, S. A. consideró demasiado tentador para resistirse a él[71].

Cuando un empleado de Fazio Mechanical abrió sin darse cuenta un mensaje de correo electrónico de *phishing* con un archivo adjunto infectado con *malware* (una variante del troyano Zeus para la banca producido por Crimen, S. A.), no sólo infectó su ordenador, sino también el resto de los de la empresa. Además, puesto que Fazio estaba conectado a la red de Target, el troyano también permitió a los *hackers* asomarse a la red de su presa última: el minorista gigante Target Corporation. El resultado fue el ataque contra Target mencionado previamente y un robo masivo de información personal y datos de tarjetas de crédito de ciento diez millones de consumidores estadounidenses. Una vez los *hackers* se infiltraron ilegalmente en Fazio Mechanical y robaron las credenciales de inicio de sesión, pudieron utilizarlas para pescar por la red de Target hasta que encontraron oro.

Allí hallaron información sobre el portal de los proveedores de Target y datos de Target Facilities Management[72]. Y después descubrieron que aquellos sistemas no estaban segmentados y diferenciados de otros sistemas de TI utilizados por el minorista, incluidos entre ellos, por desconcertante que suene, sus sistemas de pagos y financieros. Armados con todos los datos que necesitaban, los *hackers* hurgaron cual ratas en una multitud de redes interconectadas hasta que llegaron al servidor interno de la empresa responsable de controlar las decenas de miles de terminales de punto de venta individuales donde los clientes pasaban sus tarjetas de crédito en caja. Una vez allá, los piratas informáticos instalaron un troyano de *malware* conocido como .POSRAM, que copió todas las tarjetas que se pasaron por datafonos en tiendas Target de todo el país y transfirieron en secreto los datos a Rusia, un fraude abrumador que continuó hasta que el investigador en materia de seguridad Brian Krebs sacó a la luz la noticia[73]. Sin duda, el ataque contra Target es la intrusión de mayor nivel de un sistema de climatización hasta la fecha, pero no la única.

Nos gustaría creer que el gobierno podría esforzarse más en proteger los edificios

de ataques remotos, pero las evidencias no parecen indicar que tal sea el caso, ni siquiera en aquellas instalaciones que uno pensaría que son de las más seguras. En 2011, un equipo de investigación logró infiltrarse en la red del sistema de control industrial de la Agencia Federal de Prisiones y apoderarse remotamente de las instalaciones. Descubrieron que podían desbloquear puertas de celdas individuales o todo un bloque de celdas a la vez a su antojo, aunque en las pantallas de los ordenadores de las oficinas centrales de los guardias se indicaba que seguían cerradas. También consiguieron desactivar la red de comunicaciones de la prisión, de manera que los guardias individuales no pudieran solicitar refuerzos en caso de emergencia. Aún peor, lograron «destruir las puertas» electrónicamente sobrecargando el sistema eléctrico que las controlaba y, por consiguiente, las dejaron abiertas de manera permanente para toda la prisión[74]. Aplicando estas técnicas, Crimen, S. A. estaría en disposición de liberar a compatriotas para poner en riesgo a otros reos abriendo las puertas de sus celdas para permitirles cometer ataques de represalia. Y estas amenazas no son sólo teóricas.

A mediados de 2013, un «error» informático desconocido en el Centro Correccional Turner Guilford Knight de Miami, Florida, abrió de manera simultánea y repentina todas las puertas del ala de máxima seguridad y liberó a los prisioneros[75]. Siguió un motín que permitió a miembros de bandas vengarse de sus rivales. De acuerdo con el sistema de videovigilancia de la cárcel, un preso en particular parecía preparado para aquel episodio que desconcertó a guardias y presos por igual. En el momento en el que las puertas se abrieron de manera inesperada, aquel preso avanzó caminando tranquilamente por el pasillo que conducía hasta la celda de un enemigo de toda la vida y lo «apuñaló» con un cuchillo de fabricación casera antes de regresar a su propia celda. La causa del «error» seguía en fase de investigación a finales de 2014, pero este incidente sugiere que no todos los edificios de nuestra sociedad necesitan estar conectados a Internet.

La creciente superficie de amenazas que ha comportado el advenimiento de la Internet de las Cosas crea oportunidades no sólo para Crimen, S. A., sino también para Estados nación, tal como descubrió la Cámara de Comercio de Estados Unidos. En tanto que principal grupo empresarial del *lobby* defensor de los intereses empresariales en el país, la cámara suele posicionarse con respecto a asuntos internacionales y de comercio exterior y su posición acostumbra a ser crítica con China, en apoyo de las tres millones de empresas que la integran. Pese a que la Cámara había logrado detener con éxito varios ciberataques contra su red principal procedentes de la República Popular en el pasado, su suerte se torció a finales de 2011, cuando descubrió que un termostato conectado a Internet que se había instalado recientemente en una de sus oficinas en Capitol Hill había creado en secreto una puerta trasera para acceder a su red corporativa interna[76]. Los directivos de la Cámara realizaron aquel descubrimiento al detectar que el aparato de ahorro energético había estado comunicándose en secreto con una dirección de Internet en

China.

Mas si bien los atacantes habían sido lo bastante sagaces como para utilizar el termostato para infiltrarse en la red principal de la Cámara, no demostraron ser tan diestros a la hora de canalizar sus propias tareas de impresión. Su negligencia hizo que una impresora que utilizaban los ejecutivos de la Cámara empezara a imprimir de manera espontánea páginas de información con caracteres chinos impresos, algo que los agentes del FBI consideraron una prueba inequívoca de que había algo raro. Una vez dentro de la red de la Cámara, los atacantes buscaron información presupuestaria y financiera, vulneraron sistemas de correo electrónico y se centraron en los empleados que trabajaban en asuntos de política comercial en Asia. Que nadie se equivoque: la Internet de las Cosas tiene profundas implicaciones geopolíticas y los países capaces de aprovechar estas tecnologías a su voluntad tendrán acceso a una ventaja estratégica y a una información privilegiada sin parangón. Tal como el primer ministro chino, Wen Jiabao, proclamó en un discurso pronunciado en agosto de 2009 en la ciudad de Wuxi: «Internet + Internet de las Cosas = Sabiduría de la Tierra»[77].

El sistema operativo de la ciudad inteligente

> Aquéllos versados en la guerra son capaces de reprimir al Ejército enemigo sin batalla. Capturan sus ciudades sin asaltarlas y derrocan el Estado sin necesidad de operaciones dilatadas.
>
> SUN TZU

En 1964, el mariscal McLuhan predijo, de manera clarividente, que «mediante medios eléctricos […] todas las tecnologías previas […] incluidas las ciudades […] se traducirían en sistemas de información»[78]. Han transcurrido cincuenta años, pero su predicción era de lo más acertada. La Internet de las Cosas tiene todo el potencial de transformar las ciudades en ecosistemas vivos de inteligencia ambiental y sensores conectados, lo cual mejora sobremanera la calidad de la vida para sus habitantes. En la visión utópica de las ciudades inteligentes, los cubos de basura con sensores incorporados notificarán a los basureros cuando estén llenos y éstos enviarán de inmediato al camión de la basura equipado con GPS más cercano para que se los lleve. Cada vez son más las «redes con sensores municipales» capaces de medir la contaminación que genera cada edificio, la calidad del aire en un bloque concreto o el número de peatones que transita por una calle determinada, lo cual ha dado lugar al primer «monitor de actividad Fitbit para ciudades» de la historia[79]. Dotar nuestro alumbrado público de mejores sensores permitirá a los ayuntamientos proporcionar el nivel adecuado de iluminación, ajustado a la hora del día, la estación del año y las condiciones climáticas, lo cual podría reducir los costes energéticos en hasta un 30

por ciento[80]. Eso, claro está, si todo marcha sobre ruedas.

La perspectiva menos optimista de un sistema operativo de toda la ciudad sería una red municipal de dispositivos conectados a la Internet de las Cosas, siempre activados y sujetos a ataques por parte de piratas informáticos de cualquier parte del mundo. Mediante un sistema de detección del tráfico inalámbrico implementado habitualmente en ciudades de todo el mundo, un *hacker* argentino, César Cerrudo, logró hacerse con el control de los semáforos de Manhattan manejando fraudulentamente los sensores subyacentes engastados en las carreteras, una técnica que le permitió desviar el tráfico y provocar atascos a su voluntad[81]. Infiltrarse de manera ilegal en edificios y en el sistema operativo de una ciudad podría poner en riesgo la seguridad física, además de permitir a los atacantes tomar el control de ascensores, conductos de aire, cierres de puertas, iluminación, puentes, túneles, instalaciones de tratamiento de aguas y otros sistemas vitales. Al igual que los contadores inteligentes pueden piratearse, también se pueden manipular los tendidos inteligentes, y la capacidad de un colectivo de *hacktivistas*, una banda de crimen organizado o un Estado corrupto de dejar sin electricidad a masas de ciudadanos se ha convertido hoy en una realidad[82]. En julio de 2014, un investigador en materia de seguridad logró hacerse con el control del suministro eléctrico de Ettlingen, una población de cuarenta mil habitantes situada en el sur de Alemania. Un *hacker* que hubiera aprovechado la misma vulnerabilidad podría haber desconectado todos los suministros municipales, incluidos la electricidad, el agua y el gas[83].

La creación de la Internet de las Cosas promete inmensas mejoras tanto para nuestra calidad de vida como para la economía mundial, sobre todo a medida que vaya habiendo más objetos «inteligentes» que aprendan a interactuar automáticamente entre sí en nuestro beneficio. Dejando de lado las grandes inquietudes acerca de la privacidad por el momento, con miles de millones de coches, cafeteras, edificios, teléfonos móviles, ascensores, lavavajillas y juguetes hablando entre sí y recibiendo órdenes de Internet en gran medida, hemos proporcionado a los atacantes puntos de contacto innumerables para infiltrarse en nuestras vidas y conducirlas a peor.

Ni siquiera somos capaces de proteger las relativamente pocas cosas que tenemos conectadas a Internet hoy en día y, no obstante, día tras día incorporamos nuevos objetos inteligentes a nuestros hogares y nuestras vidas, sin preocuparnos siquiera por detenernos a preguntarnos qué riesgos potenciales e inconvenientes plantean. En consecuencia, en gran medida como los practicantes de la antigua arte marcial del yudo, los atacantes ahora están en disposición de usar el peso y la fuerza de nuestras propias conexiones desmesuradas para derrotarnos. En efecto, hemos conectado el mundo, pero no hemos conseguido hacerlo de manera segura… una decisión de la que posiblemente acabemos arrepintiéndonos, sobre todo cuando empecemos a conectar nuestro propio cuerpo humano a Internet.

Capítulo 14

Cuando el objeto del pirateo eres tú

> La Internet de las Cosas, también conocida como Internet de los Objetos, lo cambiará todo… inclusive a nosotros.
>
> DAVE EVANS, exjefe del departamento de Futurismo de Cisco

«Steve Austin, un astronauta, un hombre moribundo. Señores, podemos reconstruirlo, disponemos de la tecnología para hacerlo. Estamos en disposición de crear al primer hombre biónico. Steve Austin será ese hombre. Mejor de lo que era. Más fuerte. Más rápido». Ésas eran las líneas que se narraban en los créditos de apertura de la serie televisiva de la década de 1970 *El hombre de los seis millones de dólares*. Como un montón de chavales de aquella época, me asombraba la tremenda fuerza sobrehumana que poseía el superhéroe biónico protagonista y soñaba con ser capaz de correr igual de rápido, saltar igual de alto y ver igual de lejos que él. Pero, por emocionante que fuera aquel hombre biónico, los adultos me aseguraban que todo era ficción, pura fantasía extraída de los anales más descabellados de la ciencia ficción. Sin embargo, más tarde descubrí que la ciencia ficción puede convertirse rápidamente en hechos científicos.

Conocí a Bertolt Meyer a mediados de 2012 mientras rodaba un documental para el canal televisivo Channel 4 del Reino Unido titulado *Cómo construir a un hombre biónico*. Meyer, un psicólogo social de treinta y tres años licenciado por la Universidad de Zúrich, estaba investigando tanto las posibilidades como las implicaciones éticas de las últimas tecnologías biónicas. Su interés en el tema no respondía únicamente a la curiosidad científica, sino también a su destino personal: Meyer había nacido sin el antebrazo izquierdo. De niño había utilizado diversas prótesis primitivas, todas las cuales le hacían sentir distinto y cohibido, por no mencionar la funcionalidad sumamente limitada que le aportaban. Meyer aspiraba a tener la misma funcionalidad anatómica que el resto de las personas y quería llegar más allá de las manos fijas y de los ganchos metálicos que le habían colocado de niño. En 2009, ese sueño se convirtió en una realidad cuando lo equiparon con uno de los aparatos protésicos más avanzados que existen: la mano Touch Bionics i-limb.

Meyer se había convertido así en un auténtico hombre biónico. Estaba fascinado con sus nuevas habilidades físicas, entre las cuales se incluía la posibilidad por primera vez en su vida de aplaudir, sostener un tenedor y transportar una bolsa de la compra pesada con su mano izquierda. La nueva mano biónica contaba con un chasis de aluminio que la dotaba de un diseño de «mayor durabilidad y agarre y mejor

adecuación anatómica» que las prótesis anteriores. Meyer controlaba el aparato enviando pulsaciones mioeléctricas desde la carne humana de la parte de su brazo situada justo por encima de la extremidad protésica a sensores con electrodos acoplados a su piel, lo cual le permitía abrir la mano, cerrarla, girarla y agarrar objetos. Aquello suponía un verdadero avance para Meyer en el plano personal y suscitó en él un profundo interés por el mundo de la biónica, el tema de su documental, para el cual me entrevistó.

Mientras el hombre biónico y cineasta y yo analizábamos las implicaciones técnicas de estas tecnologías, la conversación derivó hacia el tema de la seguridad digital, un aspecto que Meyer aún no se había planteado. Resultaba que los impulsos mioeléctricos del cuerpo de Meyer no eran el único modo como podía accionarse su mano biónica, sino que ésta también estaba dotada de Bluetooth y podía controlarse, ajustarse y reprogramarse mediante una aplicación móvil que se había descargado del fabricante en su iPhone. Le expliqué a Meyer las inseguridades inherentes y harto conocidas del protocolo de Bluetooth y la cantidad de veces que había sido vulnerado por los *hackers* en el pasado. De súbito, en un instante, Meyer entendió las implicaciones de su vulnerabilidad y empalideció, boquiabierto al conocer unas vulnerabilidades que nadie le había expuesto.

Le pedí a Meyer que me dejara ver su teléfono móvil y la aplicación que utilizaba para controlar su apéndice biónico. Accedió y me entregó el dispositivo. Al examinar la aplicación Bluetooth, vi que ofrecía diversas posiciones de agarre y opciones de reprogramación. Si pulsaba un botón, su mano se abriría y con otro se cerraría; era posible mover los dedos por separado y manipular el pulgar y la muñeca. Me había hecho con el control del hombre biónico y de su cuerpo. Por el simple hecho de adueñarme de su iPhone, el cuerpo de Meyer se doblegaría a mi voluntad. Por supuesto, no me hacía falta tener acceso físico a su teléfono, dado que utilizaba el protocolo Bluetooth, inherentemente inseguro. Podía limitarme a piratearlo y tomar el control de manera remota. Sin que Meyer fuera consciente de ello, su mano se había unido a la Internet de las Cosas y, al hacerlo, su uso no recaía exclusivamente en su dueño legítimo. Tras superar la conmoción inicial, Meyer y yo continuamos nuestra conversación y acabamos entablando amistad. También descubrimos una lección importante juntos. Por primera vez en la historia de la humanidad, el cuerpo humano en sí podía ser objeto de ciberataques.

«Ahora todos somos cíborgs[1]»

Cualquier persona que lleve gafas, en cierto sentido, es un cíborg.

Evgeny Morozov

El término «cíborg», abreviatura en inglés de «organismo cibernético», invoca imágenes de un mundo aterrador poblado por agresores humanoides, como los Cylons de *Galáctica, estrella de combate*, los Borg de *Star Trek* o los ciberhombres de *Doctor Who*. Pese a tratarse de un término relativamente nuevo, el hecho de corregir las limitaciones del cuerpo humano se remonta a varios milenios atrás, a los pueblos ancestrales que empleaban madera, cobre y hierro para reemplazar las extremidades perdidas o deformadas. Desde entonces, las prótesis han recorrido un largo camino, no sólo reemplazando las funcionalidades corporales parciales perdidas debido a una lesión o enfermedad, sino también superando las capacidades de equivalentes biológicos con buen funcionamiento. El caso del medallista de oro sudafricano Oscar Pistorius puso de relieve estos avances. El velocista, con ambas piernas amputadas por debajo de la rodilla, fue la diana de las quejas de otros atletas, quienes aseguraban que sus piernas artificiales le concedían una ventaja injusta.

Hoy en día, la tecnología no sólo está aumentando de manera artificial nuestras extremidades y sentidos, sino también nuestras mentes. Más del 90 por ciento de los propietarios de teléfonos inteligentes afirman tener sus teléfonos a menos de un metro de distancia, todas las horas del día, cifra que seguramente aumentará en el futuro[2]. Estos dispositivos no sólo son una suerte de cerebro externo, sino que también representan una especie de extremidades fantasma a las que estamos unidos de manera persistente y cuya ausencia, cuando nos los olvidamos sin querer o están lejos, nos produce un profundo nerviosismo. Utilizamos los móviles como fuentes de memoria externas (recuerdan los miles de números de teléfonos que nosotros somos incapaces de recordar) y como medio adicional de comunicación, a través del cual compartimos nuestros pensamientos con el planeta por vía de SMS, actualizaciones de estado, tuits y correos electrónicos. Además, cada vez llevaremos encima más dispositivos inteligentes y con el tiempo acabaremos implantándonoslos en el cuerpo, y, cuando eso ocurra, nosotros también nos conectaremos a la Internet de las Cosas. Estos ordenadores «ponibles», dispositivos médicos implantables, prótesis biónicas y exoesqueletos interactuarán con el mundo que nos rodea y nos aportarán nuevas capacidades físicas y mentales, además de monitorizar constantemente nuestra salud y aportarnos información relativa a ésta. Del mismo modo que el número de microchips incluidos en nuestros coches ha aumentado a lo largo del tiempo y se han incorporado a una única red denominada red de zona del controlador, lo mismo ocurrirá con todos los dispositivos que portemos encima y dentro de nosotros, los cuales formarán su propia red de área corporal en el futuro. Tales cambios acarrearán importantes problemas de seguridad y privacidad que afectarán a la Internet de las Cosas más amplia en general, con la excepción de que en esta ocasión los nodos de Internet seremos nosotros.

Si el futuro cíborg que nos aguarda se parece más al terror retratado por Mary Shelley en *Frankenstein* o a las posibilidades heroicas de Tony Stark en *Iron Man* aún está por ver. Pero una cosa es indudable: Crimen, S. A. ha demostrado reiteradamente

su voluntad y capacidad de aprovechar cualquier tecnología emergente en beneficio propio y piratearte a ti y tu cuerpo podría ser una oportunidad demasiado buena para dejarla pasar.

Más de lo que el ojo ve: el mundo de la informática llevable

Quizá uno de los primeros dispositivos de informática llevable que tuvo una aceptación generalizada fue el audífono, que, a lo largo de su evolución, ha pasado de ser un transistor del tamaño de una baraja de cartas que se llevaba colgado del pecho mediante unos tirantes a ser una unidad con microprocesadores digitales independiente lo bastante pequeña como para caber sin llamar la atención en el canal auditivo del usuario. No sorprende que los audífonos modernos utilicen tecnología Bluetooth y sean capaces de reproducir en directo múltiples fuentes de audio y amplificarlas para las personas con discapacidades auditivas. Mediante diversas aplicaciones para teléfonos móviles, los usuarios pueden controlar y ajustar la configuración del audífono en sus teléfonos y elegir si desean oír o no el sonido ambiente, una conversación telefónica o la música de un iPod, todo ello con sólo pulsar un botón. Sin embargo, hoy en día incluso el audífono más humilde, como los auriculares Bluetooth que lleva el público general, puede piratearse mediante una gran variedad de programas Bluetooth clandestinos ampliamente disponibles mencionados con anterioridad. Como consecuencia, no sólo es factible interceptar remotamente lo que otra persona está oyendo a tiempo eral, sino que también sería posible reproducir sonidos o ruidos directamente en los oídos de las personas con problemas de sordera. Ya se trate de música *heavy metal* o de voces amenazantes que sólo la persona que porte el aparato escucharía, estos ruidos seguramente provocarían molestias y consternaciones en la persona afectada.

Hoy en día, a los audífonos se les ha sumado un abanico de opciones adicionales de sensores, rastreadores y ordenadores que podemos llevar sobre el cuerpo. Muchos de estos avances han sido impulsados por el movimiento del «yo cuantificado», que emplea diversas metodologías para recopilar datos acerca de la vida de una persona mediante sus herramientas tecnológicas. Cada día, millones de partidarios del yo cuantificado registran todos los aspectos de sus vidas, pensamientos y experiencias mediante herramientas de autorrastreo en busca de una vida mejor mediante «la conexión a la vida». Llevan un seguimiento y calculan sus horas de sueño, peso, calorías quemadas, *biofeedback*, frecuencia cardíaca, ondas cerebrales, ritmos de electrocardiograma, felicidad y números de pasos diarios, todo ello en un esfuerzo por mejorar el rendimiento físico y mental, fácilmente recopilado mediante la

introducción de dispositivos informáticos llevables conocidos como «tecnología ponible».

Al proporcionar *feedback* mensurable recopilado por pequeños ordenadores que se llevan sobre el cuerpo, estos dispositivos permiten a las personas que están a dieta saber cuántos pasos han dado y cuánta actividad física han realizado. La información se muestra en unos tableros de mandos de diseño impecable en el ordenador, delinea claramente las tendencias de la buena forma e incluso ofrece elementos de ludificación con marcadores de mejores posiciones y asignación de medallas una vez satisfechos los objetivos predeterminados. Armadas con esta información, las personas a dieta pueden realizar cambios en su comportamiento, como comer menos o moverse más para alcanzar sus metas de pérdida de peso. Estos dispositivos también desempeñan un papel importante en la prevención de enfermedades y la mejora de la salud general.

En 2014 se vendieron en todo el mundo más de 100 millones de dispositivos de tecnología ponible y se espera que en 2018 esa cifra aumente a 485 millones de unidades[3]. Los dispositivos ponibles se engloban en varias categorías amplias, como pulseras medidoras de actividad, incluidas entre ellas la Fitbit Flex, Jawbone’s UP, Nike FuelBand; relojes inteligentes (el Pebble, el Galaxy Gear de Samsung o el Apple Watch), o incluso gafas como Google Glass. Pese a que hasta ahora la tecnología ponible había sido algo muy minoritario destinado a un nicho muy concreto del mercado, en el futuro próximo seguramente se convertirá en algo generalizado.

La mayoría de los dispositivos ponibles se sincronizan con el teléfono móvil del usuario vía conectividad Bluetooth o Wi-Fi y, cuando lo hacen, tu información de salud personal pasa a circular por la Internet de las Cosas y deviene tan fácil de piratear como otros objetos de la IoT[4]. Es más, muchas tecnologías ponibles están estrechamente integradas con redes sociales, de manera que, por ejemplo, tu monitor de actividad Fitbit puede postear automáticamente el número de pasos diarios que has dado en tu página de Facebook. No obstante, ello suscita algunas inquietudes en temas de privacidad, como pueden ser: ¿quién posee tus datos?, ¿cómo se garantiza su seguridad? y si pueden compartirse con terceras partes. Pese a ello, sorprendentemente, el 52 por ciento de las aplicaciones de *fitness* carecen de políticas de privacidad disponibles. Y, como ya hemos aprendido, la información que parece inocua puede acabar volviéndose en nuestra contra. Unos patrones de sueño pobres documentados de manera automática por tu dispositivo ponible pueden ser relevantes ante un tribunal en un juicio por un accidente de tráfico. ¿Te exigirá tu mutua de salud que te pongas un medidor de actividad para definir con exactitud sus primas, de la misma manera que las aseguradoras de vehículos están instalando cajas negras en los automóviles?

Una de las últimas tendencias en informática ponible es la incorporación de videocámaras a los dispositivos, ya se trate de la popular cámara GoPro de alta

definición y con Wi-Fi utilizada para fotografiar deportes de acción extremos o algo más sutil, como la cámara incorporada en Google Glass. Si bien la idea de que la mayoría de las personas caminen por las calles llevando unas gafas con cámara de vídeo conectadas a Internet puede parecer absurda ahora mismo, piensa que lo mismo creíamos del ordenador personal y el teléfono móvil. Google ya se ha asociado con el gigante de la visión Luxottica para incorporar sus Glass en gafas Oakley y Ray-Ban, y Deloitte ha predicho que en 2015 se venderán millones de gafas inteligentes[5]. Dispositivos como Google Glass ofrecerán multitud de comodidades técnicas, todas ellas incorporadas en un único dispositivo muy fácil de llevar, como son la capacidad de hacer fotografías y enviarlas, de grabar vídeo, de realizar llamadas telefónicas, de efectuar búsquedas en Internet, de enviar mensajes SMS y de leer el correo electrónico. Estas capacidades son el pináculo de lo que es posible en el mercado de la informática ponible actual y funcionarán mediante conexiones Wi-Fi, Bluetooth y GPS, todas ellas convenientemente atadas a los planes de datos móviles de nuestros teléfonos inteligentes. Tal como se ha indicado en capítulos anteriores, con observaciones tanto por parte del Sr. Burns de *Los Simpson* como del Sr. Chertoff de Departamento de Seguridad Nacional de Estados Unidos, la potencia y la conectividad inmensas de Google Glass acarrean también multitud de aspectos relacionados con la privacidad y la política pública. Sin embargo, también existen amenazas para la seguridad considerables que deben tenerse en cuenta.

El temor a la filmación ha conducido a prohibir el uso de Google Glass en distintas salas públicas, incluidos recintos deportivos, conciertos, vestuarios de gimnasios, bares, clubs de *striptease*, casinos, hospitales y salas de cine en el Reino Unido[6]. Entre las razones mencionadas para estas prohibiciones del dispositivo figuran desde el conteo de cartas hasta la piratería de películas de cine y el espionaje industrial. Pero existe además otro problema. Las gafas Google Glass pueden manipularse para que tomen fotografías y graben vídeo en secreto y lo reproduzcan a tiempo real y de manera tácita a Crimen, S. A. en cualquier lugar del mundo, todo ello sin el conocimiento del dueño del dispositivo. Tal como hemos visto con el *software* malicioso empleado para subvertir teléfonos móviles u ordenadores portátiles, las gafas en la Internet de las Cosas pueden activarse sin que indiquen visiblemente que están grabando.

De hecho, ya había habido *hackers* que habían vulnerado la seguridad de las Google Glass antes siquiera de que el dispositivo se pusiera a la venta al público general[7]. Los agujeros en la seguridad de Google Glass implican que el dispositivo puede manejarse de raíz y subvertirse para transmitir todo lo que ves y escuchas en tiempo real, incluidos los detalles de tus cuentas y las contraseñas mientras las tecleas para conectarte a tu banco en línea. Las funciones de GPS de Google Glass conllevan que Crimen, S. A. también podrá determinar tu ubicación precisa, por ejemplo cuando te encuentres en un cajero automático y teclees tu número secreto[8]. Y mientras que tu abuela jamás necesitó ningún programa antivirus para usar sus gafas,

es posible que tú sí lo necesites[9]. Ya se han creado diversas herramientas de *software* dañino y espía para Google Glass y, en consecuencia, por primera vez en la historia de la humanidad, también ahora tus globos oculares pueden piratearse.

Dado el ritmo al que avanza el progreso tecnológico, el hecho de portar un ordenador «voluminoso» en las gafas pronto podría resultar demasiado engorroso para la generación siguiente, por lo que muy probablemente la próxima iteración de estos dispositivos sean unas lentes de contacto con Internet[10]. Si bien Google aún no ha confirmado públicamente si está fabricando una versión en lentes de contacto de Google Glass, sí sorprendió al mundo a mediados de 2014 al anunciar que estaba trabajando en un proyecto de «lentillas inteligentes» para la Internet de las Cosas con la farmacéutica Novartis. Estas lentillas ofrecerán diversos sensores de microchips y antenas que por primera vez harán posible monitorizar de manera continua los niveles de azúcar en sangre de los diabéticos sin necesidad de los dolorosos pinchazos que emplean los sistemas de comprobación de glucosa actuales. Este dispositivo se halla aún en sus estadios iniciales con la Administración de Alimentos y Medicamentos (FDA por sus siglas en inglés, de Food and Drug Administration[11]). Para no quedar rezagada, Samsung está desarrollando sus propias lentes de contacto con Internet, las cuales mostrarán todos los datos web actualmente disponibles con las gafas de Google, pero en formato lentilla, utilizando unos diodos emisores de luz montados y una mezcla de nanocables de plata y grafeno[12]. Ahora bien, por muy avanzada que la informática posible prometa ser, existe aún una frontera más lejana en la búsqueda de la integración plena entre hombre y máquina: la implantación de ordenadores en el propio cuerpo.

Me estás rompiendo el corazón: los peligros de los ordenadores implantables

La primera vez que se implantó con éxito un dispositivo médico electrónico en el cuerpo humano fue en 1958. Fueron dos cirujanos suecos quienes realizaron aquella operación histórica en Arne Larsson, un ingeniero que vivió cuarenta y tres años más, toda una vida de recuerdos y experiencias que no habría disfrutado de no ser por el ordenador del tamaño de una pelota de *hockey* que le instalaron en la cavidad abdominal y hacía que su corazón latiera con normalidad[13]. Hoy, casi sesenta años después, el mundo de la medicina ha dado pasos de gigante en el abanico de las capacidades de los dispositivos médicos implantables (DMI). Estos dispositivos han registrado múltiples mejoras en portabilidad, duración de la batería y eficacia, y hoy en día transmiten de manera remota al médico de un paciente información esencial a través de Internet. El primer marcapasos Wi-Fi de Estados Unidos se implantó en el

pecho de Carol Kasyjanski, de Roslyn, Nueva York, en 2009, y una vez completada la cirugía, su corazón latente se convirtió en el primero en unirse a la Internet de las Cosas[14].

Además de marcapasos, hay otros muchos DMI de uso común en el mundo actual, incluidos entre ellos desfibriladores implantables, bombas diabéticas, implantes cocleares y neuroestimuladores. Si bien cada aparato tiene su cometido terapéutico dentro del cuerpo, los DMI se comunican con el mundo exterior a través de protocolos de radiofrecuencia habituales como Bluetooth, Wi-Fi, NFC y RFID. Millones de estadounidenses llevan DMI y cada año se implantan dispositivos inalámbricos en aproximadamente 300 000 pacientes nuevos[15]. Estos dispositivos se han convertido en una medicina moderna ubicua, gracias a su tamaño cada vez más reducido, a sus capacidades mejoradas y a los beneficios clínicos manifiestos que aportan. Los dispositivos médicos inalámbricos, como los desfibriladores cardioversores implantables (DCI), permiten a los médicos monitorizar de manera remota la frecuencia cardíaca y los electrocardiogramas de sus pacientes en tiempo real y, por ende, reducen enormemente la necesidad de costosas visitas a la consulta. En caso de detectar alguna anomalía en el DCI, los médicos contactan de inmediato con sus pacientes y les notifican que acudan a la consulta para someterse a tratamiento. El inmenso potencial para salvar vidas que representan estos avances no debe pasarse por alto, pero a medida que vayamos integrando las tecnologías de la información en nuestra propia biología, cada vez serán más las personas que pasen a formar parte de la nación cíborg, con implicaciones relevantes para su salud, privacidad y seguridad.

Los dispositivos médicos estropeados son una de las principales causas de lesiones graves y mortalidad en Estados Unidos y el número de aparatos retirados del mercado se ha duplicado entre 2004 y 2014[16]. Cerca del 25 por ciento de estas retiradas del mercado se debieron a fallos relacionados con la informática, y el 94 por ciento de ellos «planteaban un riesgo entre medio y alto de graves consecuencias para la salud»[17]. Incluso en los hospitales se ha detectado que una amplia variedad de aparatos terapéuticos, como máquinas de resonancias magnéticas (MRI), radiografías y anestesia, bombas de infusión intravenosa, tomografías axiales computerizadas (TAC) y ventiladores estaban plagados de virus informáticos y los *hackers* podrían haber aprovechado sus vulnerabilidades de manera remota con facilidad[18]. De hecho, en 2013, el Departamento de Seguridad Nacional de Estados Unidos emitió una alerta que avisaba a las instalaciones médicas de que más de trescientos dispositivos de cuarenta fabricantes distintos presentaban vulnerabilidades que podían ser explotadas por los malhechores[19]. Resulta que, igual que un ordenador Windows o un iPhone pueden bloquearse, también lo puede hacer un aparato médico del cual depende tu vida. Ahora bien, existe una diferencia importante con los DMI. En contra de lo que ocurre con el teléfono inteligente, no es posible descargarse nuevo *firmware* por el aire para un marcapasos, sino que los cirujanos tienen que

abrirte de nuevo el pecho o el abdomen y obtener acceso físico al dispositivo para actualizar o sustituir debidamente el *firmware*.

Más preocupante quizá sea el hecho de que cuantos más ordenadores diminutos nos implantemos dentro del cuerpo para monitorizar y mejorar nuestra salud, más oportunidades creamos para que otras personas se cuelen en nuestras entrañas y subviertan esta máquinas con fines viles. Muchos dispositivos médicos se venden sin ningún mecanismo de seguridad incorporado. En su lugar, los fabricantes de DMI, como otros objetos conectados a la Internet de las Cosas, tienden a confiar en la seguridad por omisión… al fin y al cabo, ¿quién iba a querer *hackear* un marcapasos? Esta lógica imperfecta desatiende el hecho de que existe una minoría muy reducida de personas crueles y odiosas en el mundo que serían capaces de demostrar sus proezas técnicas sin importarles el prójimo. Así ocurrió en 2008, cuando unos piratas informáticos alteraron el sitio web de la Fundación para la Epilepsia estadounidense e incluyeron centenares de imágenes animadas a ritmo acelerado, las cuales provocaron violentos ataques entre los epilépticos que, inocentemente, visitaban el sitio web en busca de asesoría médica[20].

Un equipo de investigación de las universidades de Massachusetts y Washington demostró asimismo que la amenaza contra los dispositivos médicos era harto real cuando logró poner en riesgo la seguridad inalámbrica del marcapasos y desfibrilador del corazón combinado de Medtronic. Tras acceder sin autorización al aparato, los investigadores no sólo lograron leer información confidencial de los pacientes, sino algo mucho más alarmante: también fueron plenamente capaces de proporcionar descargas de electricidad a un corazón que funcionaba normalmente, un acto que habría resultado letal para el desafortunado inocente[21]. Para los *hackers*, los DMI representan un nuevo rasero irresistible mediante el cual medir sus talentos y este tema figura entre los más populares en la conferencia anual de piratería informática Black Hat que se celebra en Las Vegas. Un *hacker* célebre, Barnaby Jack, tuvo un éxito considerable al lograr subvertir toda una gama de dispositivos IoT, desde cajeros automáticos hasta marcapasos. En 2012, Jack descubrió graves fallos de *software* en los DMI producidos por varios fabricantes, gracias a los cuales pudo hacerse con el control de los dispositivos. Desde quince metros de distancia y con ayuda exclusiva de su ordenador portátil, el pirata informático fue capaz de ordenar de manera remota a un desfibrilador implantado que generara una descarga de 830 voltios directamente al corazón de una persona, una descarga tan potente que sin duda podría matar a cualquier persona con un marcapasos implantado[22].

Temeroso del profundo riesgo que suponía un ataque de estas características, el cardiólogo del exvicepresidente de Estados Unidos Dick Cheney modificó físicamente el DCI de su paciente para eliminar sus capacidades inalámbricas por si los terroristas intentaban enviar una descarga letal al ya enfermo corazón del comandante en jefe[23]. En un caso en el que el arte imita la vida, la serie televisiva de Showtime, ganadora de varios Emmy, *Homeland* retrataba de manera memorable una

versión ficticia pero enteramente viable de un ataque de esta índole, cuando el terrorista Abu Nazir dirige el asesinato del vicepresidente de Estados Unidos a través de Internet vulnerando el desfibrilador cardíaco que éste lleva implantado. Ahora bien, los marcapasos no son los únicos DMI inalámbricos que los *hackers* han pirateado. Cientos de miles de personas en Estados Unidos dependen de bombas diabéticas, un dispositivo que dispensa insulina en cantidades cuidadosamente controladas a quienes necesitan ayuda para regular sus niveles de glucosa en sangre[24]. Una vez más, el talentoso Mr. Jack demostró su valía técnica y derrotó la débil seguridad que protegía algunas de las bombas diabéticas más populares en el mercado. Con una antena de radio especial que él mismo diseñó, Jack logró localizar y poner en riesgo todas las bombas de insulina en un radio de noventa metros, provocando que el suministro de insulina para cuarenta y cinco días contenido en el dispositivo se liberara de manera instantánea y de golpe, un ciberataque remoto que sin duda alguna resultaría mortal en ausencia de un tratamiento inmediato[25].

Pese a que no se han revelado ataques criminales contra DMI hasta la fecha, podemos prever que Crimen, S. A. acabará volviendo su atención hacia estos dispositivos. De hecho, la Europol, el organismo policial europeo, predijo que los asesinatos online mediante DMI podrían convertirse en una realidad a finales de 2014[26]. Algunos de estos incidentes podrían devenir potencialmente en ciberataques comunes y corrientes, pues del mismo modo que un ataque con *botnets* programados puede asumir el control de tu ordenador y tu teléfono móvil (e incluso de tu frigorífico, tal como hemos visto en el capítulo anterior), también podría hacerse con tu marcapasos. Los dispositivos médicos pirateados podrían aparecer como cualquier otra dirección IP disponible en la Internet de las Cosas y, una vez que tu desfibrilador o bomba diabética implantados se han infectado, el *spam* para cuyo envío se han destinado podría agotar la limitada y valiosa vida de la batería que necesitas desesperadamente para regular tu frecuencia cardíaca y dosis de insulina, y requerir por ende una intervención quirúrgica para su sustitución.

Huelga decir que tramas más siniestras incluso serán posibles cuando las cifras de dispositivos médicos conectados en línea se incrementen de manera exponencial. De hecho, surgirán nuevos modos de cometer asesinatos a distancia infiltrándose ilegalmente en aparatos médicos inseguros, lo cual nos adentrará en la temible era de los ciberdelitos médicos. Y pese a que un ordenador portátil no pueda disparar a bocajarro, en el mundo actual se trata de un dispositivo capaz de asesinar de todas maneras. Crimen, S. A. también buscará nuevos modos de monetizar los ataques contra los DMI. Del mismo modo que *ransomware* como CryptoLocker puede destruir el disco duro de tu ordenador o teléfono móvil y hacer que quede inservible, no sería descabellado esperar una extorsión similar contra dispositivos médicos. «Tienes sesenta minutos para transferir 10 000 dólares en bitcoins a esta cuenta o le emitiremos una descarga de 830 voltios a tu corazón». Tic, tac, tic, tac. O peor aún, piensa en las ramificaciones si los *hackers* llegaran a infiltrarse en los sistemas de

control industrial de la fábrica donde se producen los desfibriladores implantables e insertaran vulnerabilidades de día cero en los dispositivos. Estas alteraciones minúsculas del *software* podrían pasar desapercibidas durante meses o años, hasta que cientos de miles de dispositivos se hubieran implantado en pacientes de todo el mundo. Sería entonces cuando Crimen, S. A. podría perpetrar el primer asalto a una infraestructura crítica de esta índole y utilizar las tecnologías de la información para atacar a la propia biología humana, exigiendo un rescate millonario para impedir una crisis mundial. No habría modo humano de intervenir quirúrgicamente a las miles y miles de personas que llevaran una bomba de relojería literal en sus pechos en un lapso de tiempo razonable, lo cual no dejaría más alternativa que acceder a las exigencias de los delincuentes.

A tenor del ritmo de la ley de Moore, podemos esperar que los dispositivos médicos implantables se reduzcan cada vez más de tamaño y aporten unos beneficios médicos asombrosos a los pacientes. Por ejemplo, un equipo de ingeniería biomédica de la Universidad de Stanford incluso ha creado un dispositivo robótico inalámbrico y sin batería tan pequeño que puede nadar por el torrente sanguíneo, emitir diagnósticos e incluso realizar microcirugía[27]. Bienvenido al mundo de la medicina a lo *Star Trek*, si bien estos nuevos tratamientos milagrosos quizá afrontarían amenazas por parte de los *hackers*, que podrían falsificar los resultados para que se liberasen medicamentos en el torrente sanguíneo cuando no se debiera o microrrobots que atacaran tejidos sanos en lugar de un tumor en el caso de un cáncer. Si se vulnerasen estos ordenadores ingeribles e inyectables, ¿quién iba a saberlo? ¿Qué evidencia detectable, de existir alguna, dejarían como rastro?

Cuando alguien con un DMI fallece, el médico forense encargado de determinar la causa de la muerte afrontará múltiples cuestiones: ¿ha sido una muerte accidental provocada por un mal funcionamiento de un DMI? ¿Se había manipulado el dispositivo específicamente con fines criminales? ¿O se ha tratado de un suicidio en el que el paciente ha subvertido su propio DMI para poner fin a su sufrimiento, con la esperanza de que su familia reciba los fondos de su seguro de vida por su aparente muerte natural? A medida que la medicina moderna evoluciona y proliferan los DMI, es preciso formularse una pregunta vital: cuando un cuerpo tecnológicamente mejorado aparezca en la morgue, ¿quién estará capacitado para realizarle la autopsia? Los médicos y forenses carecen por completo de formación en medicina forense informática[28]. Entonces, ¿cómo serán capaces de establecer la causa de la muerte? No podrán hacerlo, y la amenaza que plantea la inseguridad de los dispositivos médicos implica que, en el futuro, incluso sería posible salirse de rositas tras cometer un homicidio.

Cuando Steve Austin y Jaime Sommers se infectan

> Un *smartphone* enlaza los ordenadores del paciente y el doctor, que a su vez están conectados a Internet, que a su vez está conectada a otro *smartphone* en otro lugar. Los nuevos dispositivos podrían colocar la gestión de los órganos internos de las personas en manos de cualquier *hacker*, timador online y vándalo digital sobre la faz de la Tierra.
>
> CHARLES C. MANN

Poco después de que el público televisivo de la década de 1970 se enamorara de Steve Austin, el astronauta reconstruido protagonista de *El hombre de seis millones de dólares*, el actor recibió una compañera mujer llamada Jaime Sommers, la primera mujer biónica del mundo. Y aunque ambos se enfrentaron y derrotaron a villanos variopintos, ninguno de ellos intentó nunca boicotear a los superhéroes poniendo en riesgo los circuitos electrónicos de sus apéndices biónicos. ¿Por qué no? Quizá porque los virus informáticos y las tecnologías inalámbricas no formaban parte del *zeitgeist* del momento, si bien, tal como vimos con Bertolt Meyer, cuando una mano, brazo o pierna se controla de manera inalámbrica y a través de Internet, como todos los objetos de la Internet de las Cosas puede convertirse en diana de los *hackers*. Pese a ser relativamente inusitadas en nuestros días, las prótesis biónicas se multiplicarán sobremanera en los años venideros, sobre todo espoleadas por las desgraciadas necesidades de los miles de soldados jóvenes regresados de Irak y Afganistán con graves heridas de guerra.

En respuesta a ello, el Pentágono y la Agencia de Investigación de Proyectos de Defensa (DARPA por sus siglas en inglés, de Defense Advanced Research Projects Agency) han lanzado el programa Revolutionizing Prosthetics, una inversión de cien millones de dólares con más de trescientos científicos implicados cuyo fin es transformar por completo el mundo de la biónica[29]. Uno de estos triunfos ha sido la prótesis Luke Arm/DEKA del inventor Dean Kamen, que debe su nombre al brazo robótico que implantan a Luke Skywalker en *La guerra de las galaxias*. El dispositivo se controla mediante las señales eléctricas que emiten electrodos conectados a los músculos de quien lo lleva y es tan preciso que es capaz de agarrar una moneda dejada plana sobre una mesa. Existen otros proyectos en curso, incluido el Human Bionic Project del MIT, que cataloga un «depósito de todos los miembros de sustitución aprobados por la FDA para amputados, lo cual les facilita encontrar el mejor modo de reconstruir sus cuerpos»[30]. Incluso se han creado órganos biónicos implantables, como páncreas biónicos, para ayudar a los diabéticos a regular sus niveles de glucosa, convenientemente gestionados mediante una aplicación en sus teléfonos móviles que se conecta de manera inalámbrica al órgano biónico[31].

Otro campo de la biónica que está evolucionando de manera rápida es la comercialización de exoesqueletos o robots ponibles, como el sistema Ekso Bionics, que, cuando se lleva de manera externa, permite a las personas paralizadas a causa de un ictus, una lesión en la médula espinal o una enfermedad, volver a caminar. El traje exoesquelético sostiene a quienes no pueden caminar y mueve por ellos sus

extremidades, lo cual permite que poco a poco sean capaces de sostenerse en pie y ambular. También las personas sin discapacidades físicas pueden utilizar los diseños de Ekso, que les proporcionan un tremendo apoyo y fortaleza aligerando la carga de su musculatura y, por ejemplo, permiten a los soldados recorrer largas distancias transportando cientos de kilos de peso sin cansarse. Los estudiantes de posgrado del Interactive Telecommunications Program de NYU incluso han desarrollado «un API de código abierto que te permite mover el brazo de otra persona de manera remota utilizando un teclado, un *joystick* o incluso un iPhone», con la finalidad de ayudar a las personas con parálisis o un control limitado de sus extremidades a funcionar con normalidad. El resultado es un control corporal no autónomo, que permite a otras personas controlar tu brazo o pierna a través de la Red[32].

Por descontado, el futuro de la biónica no estará limitado a restaurar la capacidades humanas perdidas a causa de una enfermedad o lesión. La oportunidad de mercado de mucho mayor alcance se centrará en potenciar las capacidades humanas y en brindarnos unos poderes que no hemos tenido nunca y aumentar otros que ya teníamos. ¿A quién no le gustaría tener los poderes sobrehumanos imaginados por el Tony Stark de *Iron Man*? Ahora bien, nuestra capacidad creciente de transformar el cuerpo humano mejorando nuestra propia biología a través de la tecnología de la información plantea multitud de riesgos y cuestiones éticas que deberán ser abordadas en el futuro. Sin lugar a dudas, tus piernas robóticas podrían contraer un virus y tu mano biónica podría piratearse, pero ¿qué sucederá cuando los exoesqueletos robóticos estén al alcance de cualquiera y los ladrones empiecen a utilizar una fuerza sobrehumana para robar? Imagina el futuro de los enfrentamientos entre bandas callejeras cuando tanto los Crips como los Bloods tengan acceso a estas herramientas y empiecen a enfrentarse en las calles de tu ciudad o cuando Crimen, S. A. envíe a un sicario con exoesqueleto a la puerta de tu casa para cobrar la deuda de juego que debes. Aunque estos escenarios pueden parecer fantásticos, existe una larga tradición de tecnología militar que con el tiempo ha sido adoptada por el público general, ya sean armas de fuego, gafas de visión nocturna, navegación por GPS o incluso la propia Internet. En el futuro, es evidente que los *hackers* tendrán múltiples modos de aprovecharse de los avances presentes y futuros tanto de la informática ponible como implantable. No obstante, hay otros modos en los que nuestra biología se está utilizando con fines de identificación y seguridad, y éste será el próximo campo de batalla para hacerse con el control de nuestros cuerpos y de nosotros.

Crisis de identidad: piratear la biométrica

Tendemos a pensar en nuestro rostro, ojos, voz, dedos, frecuencia cardíaca, piernas y

palmas de la mano como elementos únicos de nuestra propia biología y anatomía que nos pertenecen a nosotros y sólo a nosotros de manera incuestionable. Ojalá eso fuera verdad. Tanto si somos conscientes de ello como si no, compartimos volúmenes cada vez más grandes de información acerca de nuestros rasgos físicos y de comportamiento con el prójimo. Estos identificadores biomédicos son características físicas diferenciadoras, la más habitual de las cuales es la huella dactilar estándar, que la policía utiliza desde hace más de 125 años para identificar a los delincuentes.

Durante más de un siglo, el análisis de huellas dactilares biométricas sólo podían realizarlo de manera manual técnicos humanos especialmente formados para ello. Pero los tiempos están cambiando y los rápidos avances en la potencia de los procesadores de datos y la tecnología de sensores implican que hoy en día los ordenadores también pueden encargarse de realizar identificaciones biométricas. Como consecuencia, los sistemas biométricos están proliferando y se están volviendo mucho más frecuentes en nuestras vidas cotidianas. La biométrica cambiará fundamentalmente el modo de identificarnos en el futuro. A diferencia de las formas tradicionales de identificación, que obligan a llevar encima algo, como el permiso de conducir o el pasaporte o a recordar algo, como tu contraseña o número secreto, la biométrica es algo que siempre llevas encima y que no debes preocuparte de olvidar nunca. Porque la biométrica eres *tú*.

Los sistemas de identificación biométrica utilizan sensores informáticos para medir cosas como los surcos de tus huellas dactilares, la distancia entre tus rasgos faciales o el tono y la calidad de tu voz. Toda esta información se traduce a unos y ceros para poder ser comparada, clasificada y reidentificada, de manera que tu conjunto de huellas dactilares concreto pueda cotejarse con una base de datos de centenares de millones de otros conjuntos en cuestión de segundos. Dado el descenso de los costes y las crecientes capacidades, se espera que la biométrica se convierta en un mercado global de 23 000 millones de dólares en 2019 y que en 2018 haya ya unos 500 millones de sensores biométricos potenciales unidos a la Internet de las Cosas[33]. La biométrica será algo masivo, estará por doquier y el movimiento ya ha dado comienzo.

En la actualidad, los clientes de las cadenas de gimnasios 24 Hour Fitness utilizan sus huellas dactilares para identificarse a la entrada del club. Y los pacientes del centro médico de la Universidad de Nueva York ya no necesitan llevar sus tarjetas de la mutua encima, porque el hospital ha registrado a más de 125 000 personas en su sistema PatientSecure, que emplea un escáner biométrico especial para medir los patrones de venas únicos en la palma de la mano como medio principal de identificar a los pacientes. Ahora bien, si los hospitales no son capaces de mantener a raya el *malware* en sus máquinas de MRI, ¿por qué deberían proteger mejor tu información biométrica? Y ¿realmente es buena idea que el personal de tu gimnasio (que seguramente no tiene ninguna experiencia en seguridad biométrica) tenga acceso a tus huellas dactilares?

Los escáneres biométricos que vemos en las películas de espionaje de Hollywood como *Misión: imposible* parecen ser de tecnología tan puntera y tan sofisticados — escáneres de ojos, lectores de huellas dactilares y sistemas de reconocimiento facial — que distinguen a la perfección a los amigos de los enemigos. Con una prensa como ésta, es fácil entender por qué los sistemas de autenticación biométrica son imposibles de derrotar. Pero resulta que la biométrica no es tan segura ni infalible como suele pensarse, y un informe de 2010 del National Research Council concluía que tales sistemas son «inherentemente falibles»[34]. No sólo es posible copiar ciertos marcadores biológicos, sino que las bases donde se almacenan los datos (las representaciones digitales de tus ojos, rostro y dedos), como cualquier otro sistema de información, también pueden vulnerarse. Riesgos aparte, tanto el gobierno como el sector privado se apresuran a estrujar cualquier ventaja posible en materia de seguridad o beneficio económico de la recopilación de tus datos biométricos, datos que pueden reunirse sin tu permiso ni conocimiento.

La base de datos de identidad biométrica gubernamental más extensa del mundo está gestionada por el gobierno indio. El proyecto, conocido como Aadhaar (que significa «fundación») constituye un intento ambicioso de capturar, fotografiar y escanear las huellas dactilares y los iris de los 1200 millones de ciudadanos del país. Más de 500 millones de nacionales indios ya han recibido sus números de identificación Aadhaar y sus datos biométricos ya se han guardado convenientemente en una base de datos nacional[35]. Para no quedarse atrás, el gobierno estadounidense ha dedicado recursos significativos en el Departamento de Seguridad Nacional, el Departamento de Defensa y el Departamento de Justicia, cada uno de los cuales ha establecido amplios programas biométricos en el mundo posterior a los atentados del 11-S.

A pesar de que el hecho de que el gobierno recopile una base de datos biométricos nacional podría sonar a disponer de una herramienta útil para atrapar delincuentes y terroristas, también comporta sus propios riesgos en materia de privacidad y seguridad, tal como el gobierno de Israel descubrió en 2011. Las autoridades del país de Oriente Próximo anunciaron que se había robado su base de datos biométricos nacional íntegra, incluidos los nombres, números de la seguridad social, miembros de familia, detalles de adopción, fechas de inmigración e historiales médicos de nueve millones de israelíes[36]. Fue un contratista quien hurtó esta información que posteriormente vendió a Crimen, S. A. y acabó publicada online en la clandestinidad digital[37]. Las oportunidades evidentes en materia de fraudes, usurpación de identidad y aspectos de seguridad son manifiestas.

Gartner calcula que, en 2016, el 30 por ciento de las empresas utilizarán identificación biométrica con sus empleados[38]. A finales de 2015 se incorporarán sensores biométricos en los teléfonos móviles de última generación y, en 2018, se calcula que 3400 millones de usuarios de teléfonos inteligentes desbloquearán sus teléfonos con sus dedos, rostros, ojos y voces[39]. La biométrica es el futuro de la

identidad, la seguridad y la autenticación. Reemplazará a la contraseña habitual, que, como hemos visto a lo largo de todo este libro, es fácil de piratear, puede robarse por millones y ha sobrevivido a su tiempo de vida útil.

La seguridad biométrica ofrecerá múltiples ventajas; mientras que se te puede olvidar la contraseña o el permiso de conducir, siempre llevarás contigo tus huellas dactilares. Mas si bien la biométrica solucionará algunos problemas, también creará otros nuevos. En la actualidad, si se es uno de los diez millones de víctimas afectadas por la usurpación de identidad, es posible obtener una nueva tarjeta de crédito o incluso un número de la Seguridad Social. Y si te piratean la cuenta de Facebook o tu cuenta bancaria, puedes redefinir la contraseña. Pero, cuando te roban las huellas dactilares, no hay reinicio que valga. Son marcadores identificativos permanentes y, una vez usurpados por los *hackers*, perderás el control sobre ellos para siempre. Y cuando tu gimnasio, empresa de telefonía móvil y médico cuenten con todos tus datos biométricos y esos sistemas se vulneren (y no tengas duda de que se vulnerarán), remediar el problema podría resultar mucho más difícil, si no imposible. Si el futuro de la identidad pasa por la biométrica, entonces el futuro de la usurpación de la identidad implicará robar y poner en riesgo los datos biométricos, y los ladrones y estafadores ya están manos a la obra intentando sortear estos sistemas.

Dedos cruzados (y pirateados)

> Si alguien te roba la contraseña, puedes cambiarla… tantas veces como sea preciso. Pero no te puedes cambiar las huellas dactilares. Sólo tenemos diez. Y las dejamos en todo lo que tocamos.
>
> Senador AL FRANKEN

La decisión de Apple de lanzar su iPhone 5s insignia a finales de 2013 con autenticación mediante huella dactilar fue un momento trascendental para la identificación biométrica. Conocido como Touch ID, el sensor de huella dactilar incorporado podía utilizarse para desbloquear el teléfono, así como para efectuar compras en Internet. A partir del sistema operativo iOS 8, Apple ha puesto esta tecnología a disposición de otros fabricantes, lo cual te permite utilizar el dedo en lugar de unas credenciales de conexión para usar multitud de servicios y aplicaciones. La practicidad potencial de simplemente deslizar el dedo para autenticarte de manera inmediata y acceder de forma segura a multitud de servicios en línea es sin duda atractiva. En la misma línea, Samsung lanzó un escáner de huella digital con su teléfono de gama alta Galaxy S5 y, al igual que el iPhone, fue manipulado. El escáner biométrico de Samsung permitía a los usuarios de teléfonos móviles utilizar sus huellas digitales para autenticarse en servicios como la cuenta de PayPal almacenada

en el dispositivo, de tal modo que una huella dactilar robada podía abrir un monedero biométrico y realizar una transferencia de dinero no autorizada a cuentas de Crimen, S. A.[40]

El precio de los sensores de huellas dactilares se ha reducido de manera significativa a lo largo de los diez últimos años e incluso es posible adquirir algunos modelos de gama baja por unos diez dólares. El descenso de los precios conlleva que cada vez más fabricantes estén incorporando estas tecnologías de seguridad en una amplia variedad de dispositivos, incluidos ordenadores portátiles. Samsung, Dell, Lenovo, Sony, Acer y ASUS incorporan todos lectores de huellas dactilares en sus ordenadores portátiles y sugieren a sus clientes que utilicen huellas dactilares biométricas para bloquear sus ordenadores Windows e incluso encriptar sus discos duros. Lo cual suena fantástico en teoría, pero la implantación de estos datos biométricos fue pobre y los piratas informáticos pudieron ver las representaciones digitales de las huellas dactilares en texto simple y sin encriptar, lo cual hizo muy fácil falsificarlas[41]. En Crime U hay docenas de vídeos en línea que muestran cómo piratear los escáneres de huellas digitales, y Crimen, S. A. descubrió hace largo tiempo cómo piratear los dedos: amputándolos. Las mafias en Malasia, sin ir más lejos, han derrotado a los sistemas de ignición mediante reconocimiento de huella dactilar de los vehículos Mercedes S-Class amputando los dedos de los propietarios de estos coches de lujo con machetes[42]. Y pese a que tretas de este tipo pueden ser moneda corriente en series televisivas como *24*, amputar el dedo de un adversario para colarse en un edificio secreto o conectarse a un ordenador pronto podría dejar de ser necesario. Tsutomu Matsumoto, un investigador en materia de seguridad de la Universidad Nacional de Yokohama, ha concebido un método que le permite «tomar una fotografía de una huella dactilar latente (en una copa de vino, por ejemplo)» y recrearlas en un molde de gelatina. La técnica es lo bastante buena como para engañar a los escáneres biométricos el 80 por ciento de las veces[43]. Otros piratas informáticos han utilizado la plastilina de niños para crear moldes de huellas dactilares lo bastante buenos como para burlar al 90 por ciento de los lectores de huellas dactilares[44]. A medida que los controles de acceso biométrico proliferen, también proliferarán los motivos para derrotarlos.

Pese a que el gobierno y el sector empresarial se esfuerzan por convencer al público de la mejora en seguridad que ofrece la biométrica, son muchas las personas que no están convencidas de ello y sacan a relucir diversas inquietudes con respecto a aspectos de privacidad y vulnerabilidad. En Alemania en 2008 se avivó un debate público en torno a este tema cuando el jefe de las fuerzas policiales y ministro de Interior del país, Wolfgang Schäuble, empezó a abogar con fuerza por un uso más extendido de huellas dactilares biométricas[45]. En respuesta a ello, nuestros amigos del Chaos Computer Club lograron extraer la huella dactilar del ministro de un vaso de agua que había dejado atrás tras pronunciar un discurso público en una universidad local. Los *hackers* copiaron con éxito la huella y la reprodujeron en plástico

moldeado… cuatro mil veces. Las réplicas impresas se distribuyeron como regalo especial en la revista de *hackers* del club, junto con un artículo que alentaba a los lectores a utilizar la impresión para suplantar al ministro, abriendo la puerta a colocar sus huellas dactilares en escenas de delitos.

Los defensores de la seguridad biométrica argumentan que es inherentemente más segura porque nadie puede robarte las huellas dactilares (incorrecto, tal como hemos visto arriba) y porque las huellas dactilares son un atributo físico inmutable que los delincuentes no pueden alterar. Pues resulta que eso tampoco es verdad, según demostró en 2009 la ciudadana china de veintisiete años Lin *Ring*. Lin pagó 14 600 dólares a médicos chinos para que le modificaran las huellas dactilares con el fin de pasar los sensores biométricos que las autoridades de inmigración utilizan en los aeropuertos japoneses[46]. Lin había sido deportada previamente y anhelaba regresar a Tokio, algo que no habría sido posible si hubiera proporcionado sus huellas dactilares reales al aterrizar en el Aeropuerto Internacional de Narita. Para volverse a colar en el país, pagó a cirujanos chinos para que intercambiaran las huellas dactilares de sus manos derecha e izquierda, de tal manera que le volvieran a injertar la almohadillas de los dedos en las manos opuestas. El plan funcionó y fue admitida en el país. Fue semanas después, cuando intentó contraer matrimonio con su novio japonés de cincuenta y cinco años, cuando las autoridades se percataron de las extrañas cicatrices en las puntas de sus dedos. La policía japonesa informa de que los médicos chinos han creado un próspero negocio con la cirugía biométrica y que Lin era la novena persona a la cual arrestaban ese año por fraude biométrico mediante cirugía médica[47].

Huelga decir que tales medidas draconianas no serían necesarias si los *hackers* simplemente lograran interceptar los datos de las huellas dactilares del escáner biométrico conectado a la Internet de las Cosas mientras se envían desde el servidor informático para su procesamiento, algo que el investigador en temas de seguridad Matt Lewis ya ha demostrado en la conferencia de piratería informática Black Hat celebrada en Europa. Lewis creó el primer Biologger de la historia, el equivalente a un *malware* registrador de pulsaciones de teclas que, en lugar de capturar todas las pulsaciones que una persona tecleaba de manera inocente en su ordenador, podía robar de manera efectiva todos los escaneados de huellas digitales procesados en un escáner infectado[48]. Lewis demostró que este dispositivo de biorregistro le permitía analizar y reutilizar los datos que había capturado con el fin de socavar sistemas biométricos, pues le franqueaban el acceso a edificios supuestamente «seguros». Si bien es tentador creer que la autenticación biométrica es inherentemente más impenetrable que los sistemas de contraseña tradicionales, tal asunción sólo sería cierta si los nuevos sistemas se implementaran de una manera más segura. De lo contrario, son los mismos perros con distintas correas.

¿Tu contraseña? La llevas escrita en la cara

En la película de ciencia ficción *Minority Report*, Tom Cruise encarna a un agente de policía de Washington, D. C., en el año 2054. En una escena, el personaje de Cruise, John Anderton, avanza a grandes zancadas por un centro comercial donde su rostro es identificado por las vallas publicitarias interactivas, que saludan al detective por su nombre y le muestran anuncios fundamentados en su historial de compras previas. Al parecer, 2054 ha llegado antes de lo previsto. Ya que, tal como las huellas dactilares identifican de manera única a una persona, también la identifican las impresiones de rostros, los escáneres biométricos de tus rasgos faciales, como las distancias entre tus ojos, nariz, oídos y labios. Estas características biométricas no sólo pueden revelar tu identidad personal, sino que también permiten a los demás hacer un perfil de ti por género, edad, raza y etnicidad. Todos estos datos son como maná celestial para los comerciantes ansiosos por recrear la experiencia de publicidad personalizada del señor Anderton.

De regreso al mundo actual, las vallas publicitarias de Japón ya observan a los transeúntes, cotejan sus rasgos faciales en tiempo real con una base de datos NEC de más de diez mil patrones preidentificados para clasificar a las personas adecuadamente en diversas categorías por perfil de consumidor y modifican los mensajes publicitarios que muestran en tiempo real de acuerdo con evaluaciones demográficas[49]. Más allá de la publicidad, la tecnología de reconocimiento facial tiene otros muchos usos. FaceFirst, una empresa de biométrica de California, permite a los minoristas escanear los rostros de todos los clientes que entran en sus tiendas con el fin de identificar a ladrones conocidos. En caso de detectarse uno, el *software* envía inmediatamente mensajes de correo electrónico y mensajes de texto a todo el personal de la tienda con una fotografía del sospechoso para que los empleados puedan adoptar las «medidas apropiadas»[50]. Un sistema similar empleado por la cadena hotelera Hilton utiliza el reconocimiento facial para escanear los rostros de todos sus huéspedes, lo cual permite a los empleados saludarlos por su nombre, sobre todo a los miembros de la tarjeta VIP Gold[51].

Ahora bien, no sólo los anunciantes están accediendo a los datos de reconocimiento facial, sino también otros consumidores. Muchos de nosotros seguramente habremos notado la presencia de una cámara de seguridad en el bar del barrio y habremos dado por supuesto, en un alarde de ingenuidad, que el aparato está allá por si se produce un robo. Pero cuando una cámara de la vieja escuela se conecta a la Internet de las Cosas y al análisis de datos masivos, nace un nuevo y potente sensor inteligente. En 2012, una empresa de Austin, Texas, se asoció con los bares y los clubes nocturnos del lugar para tomar todas estas grabaciones «tontas» en vídeo y realizar análisis faciales en tiempo real a todos los clientes de sus locales. El resultado de ello es una aplicación denominada SceneTap, que permite a quienes gustan de

pasar un buen rato en Austin consultar estadísticas en directo sobre cada establecimiento y comprobar qué clubes nocturnos están llenos, son sexualmente mixtos y qué media de edad tiene la clientela. Por ejemplo, el cuadro de mandos de la aplicación puede indicar que el Main Street Bar & Grill está lleno al 47 por ciento; el 68 por ciento son mujeres con una media de edad de veintinueve años y el 32 por ciento son hombres con una media de edad de veintiséis. Esta aplicación tan práctica evita preguntarse en qué bar habrá más ambiente y permite a los muchachos de la fraternidad borrachos evitar con éxito los bares en los que sólo hay hombres y seleccionar aquéllos locales donde haya más mujeres jóvenes. ¿Es posible que las compras mediante aplicaciones del futuro permitan a los usuarios obtener más datos demográficos como la altura, peso y etnicidad de los clientes? Podría ser, pues no existen leyes ni regulaciones en Estados Unidos que protejan a los ciudadanos de las tecnologías biométricas invasivas ni que regulen las limitaciones de su uso[52].

Las tecnologías de reconocimiento facial han mejorado sus tasas de coincidencia de manera significativa y hoy ofrecen un 98 por ciento de precisión, una mejora del 20 por ciento entre 2004 y 2014[53]. Todas las grandes empresas de Internet, incluidas Apple y Google, han efectuado inversiones sustanciales en la biométrica facial, si bien la inversión más cuantiosa conocida es la realizada por Facebook, que adquirió la empresa novel de biométrica israelí Face.com en 2012 por poco menos de 100 millones de dólares[54]. Facebook hace tiempo que lleva a cabo reconocimiento facial en cada fotografía que cargas (algo a lo que otorgaste tu consentimiento en sus condiciones de uso de 9300 palabras). La adquisición de Face.com permitió a Facebook mejorar en gran medida su función de «sugerencias de etiquetaje», al identificar a todas las personas de las fotografías que publicas mediante algoritmos biométricos, a la par que te alienta a etiquetar a tus amigos y, por consiguiente, confirmar sus identidades biométricas para Zuckerberg. Las tecnologías de reconocimiento facial automático de Facebook han suscitado controversia, dadas sus implicaciones obvias para la seguridad, y legisladores de toda la UE han prohibido la función[55]. En cambio, en Estados Unidos no existe ninguna legislación que prohíba ejecutar el *software* de reconocimiento facial ante el inventario de productos de Facebook, y el producto, como hemos explicado previamente, eres tú. Más de un cuarto de billón de fotografías se han publicado en Facebook desde su fundación, lo cual implica que Facebook (y no el programa Aadhaar de la India) es el almacén más extenso de datos biométricos que hay sobre la Tierra, superando con creces el gestionado por cualquier gobierno del mundo[56].

Es de prever que Wall Street aumente la presión para monetizar los datos biométricos y no habrá pocos clientes potenciales, incluidos entre ellos los gobiernos. En su serie de revelaciones, el filtrador de la NSA Edward Snowden afirmó que el organismo para el cual trabajaba se había infiltrado directamente en los servidores de nueve de las principales empresas de Internet, Facebook incluido, lo cual, potencialmente, había franqueado a la comunidad de la inteligencia acceso a la mina

de oro biométrica de la empresa[57]. En una revelación aparte, Snowden divulgó que la NSA ya estaba absorbiendo millones de fotografías adicionales publicadas en Internet a diario y era capaz de procesar al menos cincuenta y cinco mil imágenes al día con «calidad de reconocimiento facial»[58]. ¿Qué podrían hacer las fuerzas policiales y los organismos de seguridad gubernamental con estos datos biométricos? En las sociedades democráticas, existe la esperanza de que se utilicen para apresar a criminales violentos y terroristas. Pero, una vez esta red de arrastre biométrica se construye, los usos que se le dan los controlan las personas en el poder. En un mundo clasificado con poca supervisión, es habitual que haya usos indebidos y, en manos de tiranos y dictadores, estas herramientas podrían convertirse en los cimientos de una distopía orwelliana al estilo de las Stasi.

Las fuerzas policiales del Reino Unido se han contado entre las primeras en poner en funcionamiento un programa de reconocimiento facial automatizado generalizado utilizando la tecnología de NEC NeoFace, que coteja los rostros de cualquier fotografía o vídeo tomado en la escena de un crimen con una base de datos de imágenes. Cuando el reconocimiento facial se combina con la densidad más elevada de cámaras de CCTV de todos los países del mundo, las cámaras que los agentes de policía llevan consigo y que graban de manera constante, y las aplicaciones de teléfonos móviles al estilo de *CSI* que son capaces de realizar tanto reconocimiento facial como de huellas dactilares sobre el terreno, todo apunta a que los días del rastreo de delincuentes de *Minority Report* ya están aquí[59]. ¿Cuán avanzada está la tecnología de reconocimiento facial? Lo bastante como para establecer una coincidencia entre tu rostro y el de tu perfil de Facebook en menos de sesenta segundos mientras caminas por la calle y saber tu número de la Seguridad Social sesenta segundos después. El programa que lo hace posible se denomina PittPatt y nació como un proyecto de investigación en la Carnegie Mellon University en la estela de los atentados del 11-S con una financiación multimillonaria a cargo de DARPA[60].

Cada vez más fuerzas policiales emplean CCTV para vigilar a grupos de personas que caminan por calles de los barrios marginales, por un estadio de fútbol o un aeropuerto, y un *software* como PittPatt puede ejecutarse en segundo plano y en tiempo real para identificar cada rostro al pasar y colocar claramente una burbuja al estilo de los bocadillos de texto de los dibujitos animados sobre la cabeza de cada una de ellas en la que figura un enlace web para consultar información adicional. Un simple clic en el bocadillo de datos puede mostrar el perfil de Facebook de la persona, su número de la Seguridad Social, su historial crediticio y fotografías del pasado que haya publicado en Internet, ya se trate de una imagen de un viaje familiar a Disneylandia, una imagen de sí misma con un Martini en las manos en la fiesta de Navidad de la oficina o su perfil de citas en Match.com. Mientras que sin duda habrá partidarios de que los cuerpos de seguridad tengan acceso a estas tecnologías de reconocimiento de imágenes avanzadas con el fin de velar por la seguridad pública,

quizá no estarían tan convencidos si estas potentes capacidades de vigilancia recayeran en manos del sector privado. Demasiado tarde.

A mediados de 2011, Google adquirió PittPatt, movimiento con el que el gigante de las búsquedas en Internet abrió la puerta a implementar la formidable tecnología de reconocimiento facial en todos sus productos, incluidos YouTube, Picasa, Google+ y Android[61]. Quizá el candidato más evidente que podría beneficiarse de la tecnología de reconocimiento facial sea Google Glass. Con esta herramienta sería posible identificar de inmediato a la tía buena o el tío bueno de una fiesta, y nunca más tendrías que preocuparte de volverte a olvidar de Comosellame del Departamento de Contabilidad. Preocupado por una posible respuesta negativa, Google ha prohibido el uso de las aplicaciones de reconocimiento facial de Google Glass por el momento, pero, con la adquisición de PittPatt, dispone de la capacidad técnica para ponerlo en práctica. Por descontado, los *hackers* han desmontado sus dispositivos Google Glass y han creado una serie de aplicaciones de reconocimiento facial, incluida la popular aplicación NameTag.

NameTag permite a los usuarios escanear los rostros de las personas que tienen delante y cotejarlos con millones de registros públicos disponibles en línea, que les facilitan el nombre y los perfiles en las redes sociales de la persona, incluidos los de Facebook, Twitter e Instagram, así como otros datos identificativos relevantes[62]. Tales aplicaciones de reconocimiento facial no son exclusivas de Google Glass y pueden utilizarse sin problemas también con la cámara del teléfono inteligente[63]. Como sucedía en *Minority Report*, actualmente vivimos todos en la era del reconocimiento facial. Como consecuencia, nadie es ya un rostro desconocido entre la multitud. De hecho, tu cara es hoy un libro abierto que cualquiera puede leer a simple vista, incluido el gobierno.

El sistema multimillonario del FBI Next Generation Identification (NGI) está integrado por 52 millones de imágenes faciales entre las que buscar, en las cuales se incluyen 4,3 millones de imágenes de personas que han solicitado que se verifiquen sus antecedentes no delictivos[64]. El NGI contiene asimismo 100 millones de registros de huellas digitales individuales, así como millones de huellas de las palmas de las manos, muestras de ADN e iris escaneados. Dicho sistema no sólo escanea fotos policiales en busca de una coincidencia, sino que también rastrea a los sospechosos identificando sus rostros entre la multitud mediante cámaras de seguridad estándares o comparándolos con fotografías públicas publicadas en Internet[65]. Por supuesto, no existe una tecnología biométrica infalible, y el tema de los falsos positivos —es decir, ser tomado por un delincuente en función de una coincidencia biométrica, cuando en realidad no existe tal coincidencia— puede tener graves consecuencias para los inocentes, tal como hemos visto antes con relación a la proliferación de las listas de terroristas más buscados y de personas que no pueden volar en vuelos comerciales[66].

Pese a que el reconocimiento facial podría antojarse la panacea para garantizar la

seguridad y el fin de la delincuencia, también tiene sus inconvenientes. Tal como es posible *hackear* los sensores de las huellas dactilares, también puede hacerse con los sistemas de impresión facial que cada vez se emplean más para desbloquear teléfonos y ordenadores o para obtener acceso a oficinas. Engañar a estos sistemas, como los de los ordenadores Lenovo o las aplicaciones con contraseña para *smartphones* como FastAccess Anywhere, es tan sencillo como sostener en alto una fotografía de la persona por la que uno quiere hacerse pasar[67]. Esa misma técnica también ha funcionado con los iris escaneados, cosa que permite a los piratas informáticos invertir la ingeniería de la información biométrica guardada en una base de datos segura y utilizarla para imprimir una fotografía de un iris lo bastante buena como para engañar a la mayoría de los escáneres oculares comerciales[68].

Otro desafío que plantean los algoritmos de reconocimiento facial es que incluso los mejores sistemas «sólo» se acercan a un 98 o 99 por ciento de precisión. Pese a que la tasa de error parece baja, esos errores tienen su importancia. Imaginemos, por ejemplo, un sistema de reconocimiento facial vinculado a una lista de terroristas instalado en el Aeropuerto Internacional O'Hare de Chicago. Con un tránsito anual de 50 millones de pasajeros, una tasa de falsos positivos del uno por ciento implica que 500 000 viajeros al año (más de 1300 al día) podrían ser detenidos o arrestados erróneamente a causa de un fallo informático. Este problema se agravaría, además, por los errores humanos a la hora de introducir los datos, tal como hemos visto con las listas de personas más buscadas existentes, lo cual conduciría a las cámaras a establecer una coincidencia correcta entre el rostro de una persona y un nombre mal escrito incluido en la base de datos de las personas más buscadas.

Las consecuencias de la identificación biométrica incorrecta podrían demostrar ser letales. El Departamento de Defensa estadounidense ha empezado a instalar funciones de reconocimiento biométrico y detección de blancos en su flota de drones. La empresa contratista de defensa Progeny Systems Corporation, en colaboración con el Ejército, ya ha desarrollado un sistema «de localización, rastreo y etiquetaje biométrico no cooperativo y de largo alcance» que se instala en los drones y permite a un vehículo aéreo no tripulado (UAV) identificar positivamente un objetivo humano usando datos biométricos antes de detonar artillería en la cabeza del objetivo[69]. En tal caso, una identificación biométrica con un falso positivo sería desastrosa. El futuro de la guerra es autónomo, con drones cazando, identificando y matando a enemigos basándose en cálculos realizados por *software*, en lugar de en decisiones adoptadas por seres humanos.

Dada la creciente ubicuidad de las cámaras y el *software* de reconocimiento facial, podemos prever que los delincuentes adopten plenamente estas herramientas y las utilicen en beneficio propio. Los pedófilos podrían utilizar la biométrica para identificar al niño del parque de juegos que les atrae. Y en el caso de los terroristas, por ejemplo de los atacantes de Bombay pertenecientes a Lashkar-e-Toiba, haber tenido instalada una aplicación de reconocimiento facial en el móvil les habría

permitido identificar al presidente del banco K. R. Ramamoorthy sin tener que jugar a las adivinanzas con su centro de mando terrorista en Pakistán para conocer su identidad.

Incluso Crimen, S. A. ha empezado a explorar las tecnologías de reconocimiento facial, de acuerdo con el inspector de la Policía Federal Australiana (AFP). En la ceremonia de graduación de cientos de nuevos reclutas en la AFP en 2011, los agentes detectaron a un hombre que destacaba entre la multitud de familiares que observaban a sus seres queridos recibir sus placas de policía. El hombre llevaba una cámara profesional con un teleobjetivo y parecía estar sacando fotografías instantáneas de los rostros de todos los graduados. Al ser detenido e interrogado, los agentes descubrieron que el fotógrafo formaba parte de una panda de motociclistas forajidos perteneciente al crimen organizado. Al parecer, estaba ejecutando un encargo de Crimen, S. A. de elaborar una base de datos de reconocimiento facial fotográfico para que otros gánsteres pudieran identificar a cualquier agente que intentara infiltrarse de incógnito para realizar una investigación encubierta en contra de su organización en el futuro[70]. Las herramientas biométricas tendrán profundas implicaciones no sólo para los policías de incógnito, sino también para los programas de protección de testigos. A cualquiera que haya tenido una vida anterior que quiera ocultar por motivos personales o profesionales podría resultarle imposible continuar con su vida, y no son sólo los rasgos físicos los que pueden delatar, sino también comportamientos imperceptibles.

Tu mejor comportamiento

> En el presente se están automatizando muchos empleos, pero ¿qué sucederá cuando ese concepto se amplíe a ámbitos muy importantes de la sociedad como los cuerpos de seguridad? ¿Qué sucederá si se empieza a controlar el comportamiento de delincuentes y de la población en general con máquinas gobernadas por *software*? Parecen preguntas de ciencia ficción, pero no lo son.
>
> JOSÉ PADILHA, cineasta brasileño

Cuando la mayoría de las personas piensan en la biométrica, suelen pensar en la medición de rasgos anatómicos como dedos, rostros, manos u ojos. Sin embargo, hay otra categoría de la biométrica conocida como «biométrica del comportamiento», que se ocupa de medir los modos como nosotros y nuestros cuerpos actuamos y nos comportamos en tanto que individuos, rasgos que pueden ser tan reveladores como las huellas dactilares. El ritmo y la velocidad a los que tecleamos en el teclado, la voz, los andares, las ondas cerebrales y la frecuencia cardíaca pueden cuantificarse de manera que proporcionen firmas únicas que nos identifiquen de manera individual. De la misma manera que el uso de los datos biométricos anatómicos con fines de

seguridad, identificación y control de acceso es cada vez más frecuente, también se extenderá cada vez más el campo floreciente de la biométrica del comportamiento; de hecho, ya está sucediendo.

Empresas y centros de atención al cliente de todo el mundo utilizan ya la biométrica de la voz para marcar a los clientes de manera única por su voz. Esa grabación que escuchas cuando te tienen en la espera indicándote que «la llamada puede ser grabada por motivos de garantía de calidad» oculta el hecho de que uno de los métodos que las empresas emplean para comprobar la satisfacción con la atención telefónica recibida es mediante el tono, el tenor y el vocabulario empleados durante la comunicación. Más aún, en un esfuerzo por combatir el fraude, las empresas están construyendo inmensas bases de datos con voces grabadas de consumidores y están generando identificadores de voz únicos que puedan utilizarse en llamadas futuras para garantizar que la persona al habla coincida con el identificador vocal biométrico tomado originalmente[71]. Si las voces no encajan, se formulan a la persona que telefonea preguntas de verificación adicionales, en un proceso que no resulta del todo transparente para el público general.

DARPA está investigando técnicas de «autenticación activa» centradas en los procesos cognitivos del usuario, en sus hábitos personales y en los patrones que todos seguimos al hacer las cosas, que, en combinación, nos identifican de manera única y exclusiva. Uno de estos campos de la biométrica del comportamiento se conoce como «dinámica de tecleo», que mide las variancias con las que cada uno de nosotros teclea caracteres concretos en un teclado. Las diferencias mínimas entre cuándo se presiona cada tecla, en qué secuencia, con qué fuerza e incluso cómo cortamos y pegamos pueden servir como nuestras huellas dactilares en línea ante el mundo. Empresas como la plataforma educativa en Internet Coursera utilizan el reconocimiento del tecleo para garantizar que el mismo estudiante «asiste» a cada clase virtual antes de emitir un certificado de asistencia[72].

El producto de Watchful *Software* TypeWATCH está diseñado para ejecutarse en redes en segundo plano y monitorizar de manera constante las dinámicas de tecleo de un usuario para identificar y bloquear intentos de acceso no autorizado. Otras empresas, como la sueca Behaviometrics AB, han diseñado herramientas que detectan cómo sostiene cada usuario su teléfono móvil o tableta, en qué ángulo, el modo como teclea el teclado virtual e incluso cómo desliza el dedo y junta y separa los dedos sobre la pantalla, todo lo cual revela pausas de apenas milisegundos entre las diversas acciones. Cualquier variación de una «huella cognitiva» establecida hace saltar las alarmas en un banco y bloquea el acceso a la cuenta, uno de los motivos por los que el principal banco de Dinamarca, Danske Bank, adoptó esta tecnología[73]. Los bancos creen que las herramientas biométricas de este tipo podrían reducir los índices de fraude en hasta un 20 por ciento, de manera que puedes esperar que los términos y condiciones de tu institución o entidad bancaria sean corregidos en el futuro próximo y exijan tu consentimiento para efectuar esta monitorización tan

detallada con el fin de poder usar tu aplicación de banca en el iPhone[74].

Cada día surgen nuevas formas de biométrica del comportamiento. La pulsera Nymi utiliza un voltímetro para medir tu frecuencia cardíaca y utiliza su ritmo electrocardíaco exclusivo para desbloquear tu ordenador, teléfono inteligente, vehículo y vivienda[75]. Un equipo de científicos del National Physical Laboratory del Reino Unido ha creado el sistema de reconocimiento de andares que puede utilizarse en combinación con los monitores de los CCTV para identificar de manera única a una persona por su modo de caminar[76]. Pero existe aún un modo más fácil de identificarte por tu manera de caminar: utilizando el acelerómetro del teléfono inteligente que llevas encima las veinticuatro horas del día, de manera que compartes esta información con tu empresa de telefonía móvil, el fabricante del dispositivo y los desarrolladores de aplicaciones[77].

Y aunque hoy estas tecnologías ya se nos antojen intrusivas, lo cierto es que podrían serlo aún más en el futuro. Motorola ya se ha asociado con la empresa MC10 para «ampliar las capacidades humanas mediante tatuajes RFID electrónicos ponibles prácticamente invisibles» que pueden utilizarse para autenticación de pasaportes. Y Proteus Digital Health ha creado una píldora que puedes tomarte y, accionada mediante los ácidos de tu estómago, emite una señal de ocho bits única en tu cuerpo y convierte toda tu persona en un identificador[78]. Pese a que muchos de estos productos de seguridad biométrica ofrecen grandes promesas, los *hackers* y Crimen, S. A. no renunciarán sin más a sus intentos de enriquecerse para regresar a sus madrigueras derrotados. Lo que harán probablemente es, en lugar de limitarse a piratear tu ordenador, piratear esta Internet de Ti.

Vulnerabilidades de seguridad aparte, las tecnologías biométricas y de comportamiento biométrico conllevan una larga serie de problemas relativos a las políticas públicas y la privacidad con los que la sociedad acaba de empezar a bregar. ¿Qué significa que una persona que escriba en un teclado en cualquier parte del mundo pueda ser identificada de manera remota basándose únicamente en su modo de aporrear las teclas? La estrategia se antoja perfecta para localizar al *hacker* más buscado del mundo, pero, en cambio, es una noticia nefasta para el líder de la oposición durante la Primavera Árabe. El desafío que plantea la vigilancia biométrica, ya la apliquen anunciantes en el centro comercial de tu zona o el aparato del Estado encargado de velar por la seguridad, es que afecta a nuestro comportamiento. Cuando sabemos que nos observan, nos comportamos de manera distinta y somos más aquiescentes y más fáciles de controlar[79]. Tanto en manos de un gobierno descontrolado como de una megacorporación monopolista, las modificaciones del comportamiento por autocensura que conlleva la vigilancia omnipresente pueden desembocar rápidamente en un futuro distópico para todos. No sólo nuestros yos físicos están sujetos a esta observación persistente, sino que ahora también lo están nuestros yos virtuales.

Realidad aumentada

> A medida que avance la Internet de las Cosas, el concepto mismo de una línea divisoria clara entre la realidad y la realidad virtual se irá desdibujando, en ocasiones de manera creativa.
>
> GEOFF MULGAN, Fondo Nacional
> para la Ciencia, la Tecnología
> y las Humanidades del Reino Unido

En el cine, Tony Stark nos asombra con las capacidades de su omnipotente traje de Iron Man, que, entre sus múltiples funciones, le aporta multitud de información de realidad aumentada en tiempo real gracias a la pantalla incorporada en su casco. La tecnología de esta película se fundamenta sólidamente en la realidad. La realidad aumentada (AR) proporciona una visión directa a tiempo real de un entorno físico del mundo real a través de una pantalla informática, como la del teléfono móvil o la incrustada en Google Glass y superpone capas de datos digitales adicionales, como pueden ser imágenes, sonido, vídeo o datos de GPS a ese entorno real[80]. Algunas de las primeras aplicaciones de AR fueron las usadas en las pantallas de aviso de los pilotos de cazabombarderos, que les permitían ver información del sistema esencial en las lunas de su cabina de mandos sin tener que desviar la vista hacia el instrumental durante un combate aéreo. En la actualidad, esa tecnología ha llegado a la vida civil y fabricantes de automóviles como Mercedes-Benz y Range Rover proyectan la velocidad a la que viaja el vehículo e indicaciones paso a paso directamente en el parabrisas del vehículo. A diferencia de la realidad virtual, que puede suplantar la realidad o incluso crear un mundo enteramente ficticio, la realidad aumentada potencia la percepción de la realidad aportando datos útiles encima de las cosas que vemos en el mundo real.

La AR puede utilizarse en cualquier pantalla con cámaras y sensores incrustados, ya sea la del teléfono móvil, una tableta, unas gafas o incluso unas lentes de contacto. Se prevé que en 2017 se descarguen e instalen en dispositivos 2500 millones de aplicaciones de AR al año[81]. Las ventajas de la AR son sensacionales y las principales empresas ya nos están mostrando las posibilidades que ofrece. En un anuncio de Google, un usuario con Google Glass está a punto de descender a un metro en Manhattan cuando recibe una alerta desplegable con el logotipo de los trenes de la línea 6 indicándole que el servicio de trenes se ha interrumpido, datos que se proyectan en su campo de visión en la pantalla de las Glass. Herramientas como ésta permitirán a los viajeros de todo el mundo abandonar sus voluminosas guías de viaje y utilizar una aplicación de AR para recorrer las ciudades.

Mientras caminas por la calle, estas aplicaciones pueden superponer datos y mostrarte reseñas en Yelp de los restaurantes que encuentras a tu paso y entradas de Wikipedia sobre estatuas y edificios históricos en tu campo de visión. Por supuesto,

la AR nos bombardeará con anuncios mientras deambulemos por la ciudad, cuando Google Glass identifique todos los objetos físicos que nos rodean y coloque anuncios encima de éstos. Ikea incluso incorporó AR en su catálogo de 2013, que permitía a los usuarios tomar fotografías instantáneas de sofás u otras piezas de mobiliario con sus teléfonos móviles y superponerlas a sus propios hogares (con las dimensiones correctas) para comprobar cómo quedarían antes de efectuar una compra[82]. La AR será el modo como interactuemos con el mundo que nos rodea y la Internet de las Cosas en concreto, y nos permitirá solicitar información acerca de los objetos físicos para entender mejor su historia, el uso para el que fueron concebidos y su contexto. Conectará los mundos online y *offline* y cambiará todos los aspectos de la vida y el trabajo.

La AR planteará asimismo multitud de interrogantes acerca de la seguridad y la privacidad que deberán abordarse. Una aplicación maliciosa futura podría superponer un límite de velocidad incorrecto a una señal vial de la autopista o colocar una señal falsa donde no exista ninguna en la pantalla del parabrisas AR de nuestro vehículo[83]. O lo que es aún peor, podría mostrar que un carril de tráfico está despejado cuando en realidad no lo está y provocar un accidente cuando intentamos adelantar. Tal como se ha indicado previamente, cuanto más nos desconectemos de la realidad y aceptemos lo virtual frente a lo real, más nos expondremos a la manipulación mediante ataques del tipo «en la pantalla confiamos».

Asimismo, tal como Crimen, S. A. ha creado *software* delictivo, como Blackshades, para automatizar la delincuencia, es de esperar que en el futuro ponga en circulación también aplicaciones de *crimeware* con AR. Por ejemplo, con un iPhone o Google Glass, los *hackers* podrían ser capaces de interrogar visualmente a todos los dispositivos IoT de tu oficina o domicilio y ver en sus pantallas información acerca de cuáles presentan vulnerabilidades conocidas e incluso, quizá, ver tu contraseña con un nivel de seguridad pobre, lo cual permitiría piratear la Internet de las Cosas de un modo más sencillo incluso que en la actualidad. Las tecnologías que modifican la realidad, como la AR, abrirán la puerta a entornos virtuales más envolventes, como los sistemas de realidad virtual, que también pueden subvertirse y aprovecharse indebidamente.

El auge del *Homo virtualis*

La realidad es una mera ilusión, aunque persistente.

ALBERT EINSTEIN

De manera creciente, a medida que vamos viviendo nuestras vidas mediante avatares,

en videojuegos, mundos online y redes sociales, nuestra imagen pública en Internet da la cara por nosotros en situaciones sociales, transacciones comerciales e incluso en encuentros sexuales. Nos representa en línea las veinticuatro horas de los siete días a la semana, comprimiendo el tiempo y el espacio, e interactúa en nuestro nombre con el resto del mundo incluso mientras dormimos. La conocida diseñadora de juegos Jane McGonigal ha señalado que «la persona joven media acumula 10 000 horas de juego a la edad de veintiún años», la inmensa mayoría de las cuales jugadas mediante un avatar o personaje de juego[84]. De este modo, presenciamos el auge del *Homo virtualis*, quizá la siguiente evolución del *Homo sapiens*, una especie alejada de las limitaciones del mundo físico y volcada en la inmediatez y el potencial aparentemente ilimitado de lo virtual.

La realidad virtual (VR) utiliza ordenadores para crear entornos simulados, mundos reales e imaginados en los que podemos insertar una presencia física representativa de nosotros y nuestros sentidos. Incluso es posible recrear el sentido del tacto aplicando «fuerza, vibración y movimientos» al usuario mediante la tecnología del tacto o de la retroalimentación táctil. Tal como comentó Mark Zuckerberg después de que Facebook adquiriera por dos mil millones de dólares Oculus Rift, un casco de realidad virtual con una respuesta asombrosa, a principios de 2014: «Estratégicamente, nos interesa empezar a construir la siguiente gran plataforma de computación que vendrá tras los móviles»[85]. Herramientas como el casco Oculus Rift nos transportan en un instante a una experiencia inmersiva de una bella población de la Toscana, un asiento a pie de pista para un partido de la NBA o una batalla imaginada a la par que realista con Klingons y Romulans.

Uno de los primeros mundos virtuales fue Second Life, lanzado por Philip Rosedale del Linden Lab en 2003, que permitía a los usuarios representarse con la forma de avatares con un alto grado de personalización. En Second Life era posible trabar amistades, comprar, aprender e incluso acudir a un concierto de *rock* de U2 interpretado por los avatares reales de los componentes de la banda. Otra forma habitual de mundos virtuales son los llamados MMORPG (por sus siglas en inglés, de *Massive Multiplayer Online Role-Playing Games* o videojuegos de rol multijugador masivo en línea). Los MMORPG son videojuegos que «permiten a miles de jugadores internarse simultáneamente en el mundo virtual e interactuar. Los jugadores pueden gobernar sus propias ciudades y países, preparar ejércitos» para entrar en batalla y vivir «aventuras variadas con sus avatares». El MMORPG más importante es *World of Warcraft* de Blizzard Entertainment, que cuenta ya con doce millones de suscriptores, cada uno de los cuales paga una tasa mensual por habitar un mundo virtual. Pese a ello, por intricados y estratificados que sean estos espacios virtuales en la actualidad, Rosedale anuncia un futuro cercano en el que los avances de *hardware* y *software*, como la plataforma High Fidelity, nos presentarán el mundo virtual de la siguiente generación, un mundo virtual potencialmente tan amplio y complejo como el mundo real de hoy en día.

Con el fin de entender los mundos virtuales, debemos comprender la mentalidad y la psicología de quienes *habitan* espacios virtuales. Muchos conciben sus «segundas vidas» como «primeras vidas» y el 20 por ciento de los jugadores de MMORPG contemplan el mundo de los juegos como su «verdadero» lugar de residencia[86]. Para ellos, la Tierra no es más que «el mundo carnal», un hábitat secundario en el que la carne de sus cuerpos físicos se alimenta y duerme, mientras que la mayor parte de sus relaciones interpersonales, comerciales y sexuales tienen lugar en línea. Y si bien una abrumadora mayoría de usuarios de VR no piensan de esta manera, esa sensación podría acabar siendo habitual a medida que pasamos más y más tiempo en entornos virtuales altamente inmersivos y placenteros.

Ahora bien, esta tecnoforia tiene sus desventajas, tal como puso de manifiesto una pareja surcoreana que pasó tanto tiempo en un cibercafé de su barrio cuidando de manera obsesiva de su hija virtual en el mundo online conocido como Prius que se olvidaron de regresar a su domicilio durante días para alimentar a su hijito de tres meses de carne y hueso, lo cual provocó la muerte del bebé[87]. Pese a tratarse de un caso extremo, se ha tenido noticia de docenas de episodios de este tipo en los últimos años y sin duda sucederán otros nuevos en el futuro.

La línea entre hombre y máquina, entre online y *offline*, se desdibuja cada vez más. Cualquiera que haya jugado alguna vez a un videojuego hiperrealista en primera persona con armas de fuego como *Doom* o *Call of Duty* sabrá que la experiencia virtual provoca definitivamente cambios fisiológicos, como pueden ser taquicardia o palmas sudorosas en el fragor de la batalla. Puesto que los avatares son representaciones virtuales de nosotros mismos y habida cuenta que las personas nos pasamos miles de horas encarnando la imagen pública de nuestros avatares, nuestras psiques del mundo real cada vez se enmarañan más con nuestras representaciones virtuales. Así, lo que les ocurre a nuestros avatares deja una marca en nosotros y en los mundos virtuales es posible replicar prácticamente cualquier delito que pueda tener lugar en nuestro espacio físico. Los mundos virtuales cuentan con sus propias monedas, como los dólares Linden o el oro de *World of Warcraft*, que, como los bitcoins, pueden convertirse en «dinero real» y se han convertido en una de las dianas predilectas de Crimen, S. A., que lanza 3,4 millones de ataques de *software* malicioso diarios en busca de cuentas de juego online[88].

Por extraño que pueda sonar, los delitos cometidos por y contra los avatares son cada vez más frecuentes y, en los mundos virtuales, puedes verte sometido a cualquier cosa desde *ciberbullying* hasta usurpación de identidad[89]. Sin ir más lejos, la policía japonesa arrestó a un hombre por una serie de atracos a avatares. Incluso se ha informado de «agresiones sexuales» en mundos virtuales, como ocurrió en 2007 en un asunto investigado por la Policía Federal belga[90]. En el incidente se vio involucrada una mujer cuyo avatar infectó con *malware* un hombre a quien había conocido en Second Life. El virus informático permitió al agresor asumir el control del avatar de la mujer y agredirla sexualmente de manera violenta y gráfica. En

última instancia, el caso se investigó como un incidente de «acceso no autorizado a un sistema informático» y, aunque habrá quien lo desestime tildándolo de una «violación virtual» desmadrada, en el futuro será más difícil adoptar esta posición, dada la inmersividad creciente del espacio virtual y los traumas reales que muy probablemente estos incidentes podrían provocar. Tales episodios podrían verse exacerbados mediante el creciente número de dispositivos de retroalimentación táctil corpóreos que cada vez se conectan más a mundos en línea y, por ejemplo, permiten a las parejas utilizar la ciencia de los *teledildonics* para estimularse mutuamente a través de la Red[91]. Como cualquier otro objeto preparado para conectarse a la Internet de las Cosas, estos dispositivos podrían ser vulnerados con consecuencias impredecibles.

El auge de la VR podría no sólo tener repercusiones en la esfera de los delitos, sino también en la del terrorismo y la seguridad nacional. Un informe de 2008 presentado por el director de la inteligencia nacional de Estados Unidos sugiere que los terroristas podrían estar empleando espacios virtuales para comunicaciones encubiertas, para diseminar propaganda, formar a miembros, blanquear dinero virtual e incluso reclutar a nuevos adeptos[92]. De acuerdo con un documento de ochenta y dos páginas filtrado por Edward Snowden y publicado en el sitio web del *New York Times*, tanto la NSA como los GCHQ del Reino Unido han estado espiando a los jugadores de los mundos virtuales, incluidos *World of Warcraft*, Second Life y diversos juegos de la plataforma Xbox de Microsoft[93]. Los espías han creado avatares de incógnito con el fin de «husmear e intentar reclutar a nuevos informadores al tiempo que recopilan datos» e interceptan de manera masiva las comunicaciones entre jugadores, incluidos los 48 millones de personas que utilizan la red de consolas Xbox Live. La preocupación por el hecho de que las organizaciones terroristas puedan estar utilizando estas plataformas para recaudar fondos y reclutar a personal no carecen de fundamento[94]. Hezbolá ha producido su propio videojuego con armas de fuego en primera persona titulado *Special Force 2*, el cual se utiliza como medio de radicalización de los jóvenes yihadistas. En el juego, los jugadores obtienen puntos lanzando misiles Katyusha sobre poblaciones israelíes y ganan si se convierten en «mártires suicidas» y perpetran un atentado con éxito[95].

A medida que la realidad virtual siga mejorando de manera exponencial, las distinciones entre nuestros yos virtual y físico continuarán erosionándose. El resultado será un mundo en el que cada vez resultará más arduo distinguir dónde acaba el yo físico y dónde comienza el virtual. Ésta es la Internet de Ti, y puede piratearse de arriba abajo. A lo largo de este capítulo hemos visto numerosos ejemplos de cómo la tecnología que nos rodea se está convirtiendo en tecnología que llevamos encima y dentro de nosotros. La tecnología ponible, incrustable, ingerible e implantable implica que, en mayor o menor grado, todos hemos pasado a engrosar la nación cíborg… y, como resultado, estamos exponiendo nuestros cuerpos físicos a ciberataques por primera vez en la historia. A estos desafíos se suma el hecho de que

nuestra anatomía y fisiología puede medirse actualmente desde la distancia, con o sin nuestro conocimiento, mediante la biométrica y la biométrica del comportamiento, capaces de trazar nuestro perfil e identificarnos de manera única. Como resultado, las migas digitales han llegado al espacio físico, mientras que nosotros, nuestros cuerpos y nuestra esencia, nos integramos con el ciberespacio como nunca antes. Sin embargo, como veremos, también se está dando una integración inversa. Los ordenadores y otros tecnoobjetos inmóviles pronto dejarán atrás el mundo virtual y se nos unirán desplazándose por el espacio real. Finalmente, las máquinas están cobrando vida. Tras una larga era de hibernación, están listas para descender a nuestro mundo físico y, cuando lo hagan, traerán consigo un tsunami de amenazas para las cuales no estamos en absoluto preparados.

Capítulo 15

El auge de las máquinas: ciberdelincuencia en 3D

> Sólo cuando funcionan mal nos acordamos de lo poderosas que son las máquinas.
>
> CLIVE JAMES

Rezwan Ferdaus se crió en Ashland, Massachusetts, una población lujosa en la zona residencial de Boston. Sus padres habían emigrado desde Bangladesh en busca de una vida mejor en Estados Unidos y habían depositado grandes expectativas en su hijo, a quien habían criado en el respeto a Alá y a la fe musulmana. Tras la educación secundaria, Ferdaus se licenció en Física por la Northeastern University en 2008. Incapaz de encontrar un empleo en su campo, regresó al hogar parental. Como tantos muchachos de su edad, pasaba mucho tiempo conectado a Internet. Empezó a frecuentar sitios web islamistas radicales y visionó numerosos vídeos de Al Qaeda que invitaban a los jóvenes musulmanes a sumarse a la *yihad* contra el gran Satán: Estados Unidos.

A medida que pasaba el tiempo, el joven de veinticinco años se sentía cada vez más desilusionado con Estados Unidos y resolvió que había llegado el momento de pasar a la acción. Le comentó a un hombre de la mezquita local que quería unirse a Al Qaeda y al cabo de poco tiempo le presentaron a varios «hermanos» que podían ayudarlo a cumplir su deseo. En 2010, Ferdaus empezó a planificar su propio ataque violento contra los infieles que lo rodeaban por todas partes. Y pese a no tratarse de un pensamiento original para un terrorista, su plan de utilizar robots asesinos sí que lo era. Ferdaus adquirió tres vehículos aéreos no tripulados (VANT) o drones que pretendía cargar con explosivos C-4 y enviar volando al Capitolio y al Pentágono.

Los VANT en realidad eran aviones teledirigidos, réplicas perfectas de los cazas Phantom F-4 de la Marina a una escala precisa de 1:10 y podían adquirirse en Internet a través de sitios web para aficionados a los drones. Aquellas aeronaves eran capaces de transportar una carga de veinte kilos y alcanzaban velocidades de 250 kilómetros por hora mediante dos motores a reacción incorporados. Un operador en tierra podía teledirigirlos mediante un radiotransmisor de mano o, tal como pretendía hacer Ferdaus, volar de manera autónoma con acuerdo a una ruta de vuelo predeterminada gracias a los sensores GPS de a bordo que estrellarían cada VANT en el objetivo previsto. El plan también presentaba otras ventajas: el avión robótico podía despegar y aterrizar prácticamente en cualquier sitio y los aviones pequeños a baja altura resultan prácticamente imposibles de detectar mediante radar. Ferdaus compartió sus

planes con sus afiliados de Al Qaeda, quienes le manifestaron su apoyo más entusiasta y le ofrecieron financiación.

Con un nombre falso y una tapadera, Ferdaus encargó tres maquetas de aviones por valor de 3000 dólares cada una a distintos proveedores online. Las pagó con una cuenta PayPal que creó con un seudónimo y solicitó que entregaran los VANT en unos almacenes situados cerca de Framingham que había alquilado pagando en efectivo. Allí, Ferdaus empezó a montar en secreto los dispositivos antes de avanzar a la segunda fase de su plan: la adquisición de explosivos. Para este objetivo, sus nuevos amigos en Al Qaeda resultan sumamente útiles. Le proporcionaron diez kilos de explosivos C-4, numerosas granadas de mano y seis rifles de asalto AK-47 completamente automáticos, que ocultó en su trastero alquilado de diez por diez metros.

Ferdaus viajó a Washington, D. C., para inspeccionar de cerca sus objetivos, tomar fotografías y determinar puntos de ataque en un mapa. Decidió lanzar sus aviones desde el parque East Potomac, convenientemente situado en un punto casi equidistante de sus dos objetivos. Primero atacaría el Pentágono, enviando a dos drones desde lados opuestos del edificio, ambos dirigidos contra la cuarta planta. Ferdaus no necesitaba subir a bordo de aquel vuelo. Había construido un servomotor robótico de alta presión para sus VANT autoguiados, un dispositivo que extraería de manera simultánea las anillas de las dieciséis granadas de mano que colocaría a bordo de cada aeronave teledirigida. Programaría el robot asistente de los VANT para que actuara momentos antes del impacto y extrajera las anillas para conseguir el máximo impacto.

El plan de Ferdaus requería un ataque por tierra además del ataque con drones. Para perpetrar esta parte del plan, organizaría a dos equipos de tres personas armadas con AK-47 para que tirotearan a las víctimas inocentes que huían frenéticas de las explosiones que estaban sacudiendo sus edificios. La siguiente fase del plan exigía otro avión a reacción en miniatura guiado con precisión y controlado de manera remota cargado de explosivos C-4, cuyo objetivo sería colarse y destruir la cúpula del Capitolio, haciéndola añicos.

Ferdaus regresó a Boston y redactó un plan de su misión con un grado de detalle asombroso, el cual incluía las especificaciones de los aviones, protocolos de *software*, configuraciones de *hardware*, mapas, imágenes, diagramas, límites de carga y requisitos presupuestarios. Proporcionó el documento en un llavero USB a sus supervisores de Al Qaeda, quienes recibieron su propuesta con admiración. Le preguntaron dónde había aprendido tanto sobre robótica y drones, a lo que él contestó: «La tecnología de los VANT es muy sencilla. Es cierto que se requieren ciertos conocimientos, pero llevo construyendo este tipo de aviones desde que era un crío pequeño». Acordaron entre todos llevar adelante el plan, y Ferdaus regresó a Framingham para comprobar su alijo de armas y explosivos. Al abrir su trastero, se abalanzó sobre él un grupo de agentes especiales del FBI, que impidieron el primer

ataque terrorista con drones de la historia en suelo estadounidense.

Resultó que el musulmán a quien Ferdaus se había aproximado en su mezquita local solicitando que lo introdujera en Al Qaeda era un ciudadano honrado que contactó con la policía después de conocer su petición. Los «hermanos» que presentó a Ferdaus en realidad eran agentes del FBI de incógnito[1]. En julio de 2012, Ferdaus se declaró culpable de los cargos de intento de destrucción de un edificio federal con explosivos y apoyo material a una organización terrorista extranjera y fue sentenciado a diecisiete años de prisión. Pese a que hemos visto al Ejército utilizar drones con gran repercusión en todo el mundo, los delincuentes y terroristas son perfectamente capaces de construir y utilizar también estos dispositivos. Múltiples VANT enviados desde el parque de East Potomac a 250 kilómetros por hora por debajo de los radares impactarían en sus objetivos en cuestión de minutos y no dejarían margen de maniobra para evacuar o reaccionar. A medida que el uso de los drones y otras tecnologías robóticas se generalice, podemos esperar que los utilicen todos los miembros de la sociedad, para bien y para mal. Mientras que el 11-S 1.0 consistió en que unos seres humanos se apoderaran de aviones y los impactaran contra edificios ocupados con fines terroristas, un 11-S 2.0 podría prescindir de los humanos y, en su lugar, utilizar robots.

Nosotros, robots

> Estoy convencido de que en el futuro habrá más robots en todos los aspectos de la vida. Si en 1985 te hubieran explicado que al cabo de veinticinco años habría ordenadores en las cocinas, te habría parecido una locura.
>
> RODNEY BROOKS

A lo largo de la historia del cine y la televisión nos han presentado a los robots a través de prismas diversos. Algunos eran adorables y serviciales, como WALL-E, Johnny 5 de *Cortocircuito* y C-3PO y R2-D2 de *La guerra de las galaxias*. Otros, en cambio, eran peligrosos y pretendían destruir la humanidad, como Gort de *Ultimátum a la Tierra* y los T-800 de *Terminator*. Merced a los avances de la ley de Moore, los robots están abandonando el celuloide para unirse a la realidad. El progreso exponencial de los chips de silicona, los sensores digitales, la informática en la nube y las comunicaciones de ancho de banda alto implican que los robots, al igual que los ordenadores y los teléfonos móviles antes que ellos, pronto serán omnipresentes en nuestras vidas.

Cada vez se los dota de dispositivos más avanzados, como cámaras de alta definición, sensores táctiles y telémetros láser, todos ellos unidos y ejecutados por cerebros informáticos. Los robots se mueven gracias a motores de accionamiento o

servomotores, unos motores eléctricos conectados a marchas que accionan y mueven sus ruedas, piernas y brazos, tal como los músculos mueven a los seres humanos. La revolución de los teléfonos inteligentes ha propiciado inmensas mejoras en el campo de la robótica, lo cual se explica porque los robots dependen de muchos de los mismos chips informáticos, baterías y sensores que incorpora el teléfono móvil cada vez más potente que llevas en el bolsillo.

Hasta ahora, los robots se han utilizado ampliamente en fábricas para llevar a cabo tareas repetitivas que son «peligrosas, sucias o aburridas», como las de las cadenas de montaje automovilísticas. En el presente, no obstante, se están sofisticando y se los está dotando de una destreza, unos sentidos y una inteligencia mejorados, lo cual les permite desempeñar tareas más complejas. Caminan, hablan, bailan, interpretan nuestras expresiones faciales y responden a nuestras órdenes verbales. Hay robots que cuidan de ancianos, detonan bombas, conducen coches, trabajan en la Estación Espacial Internacional (ISS) y abaten terroristas en todo el mundo. En los años venideros, apagarán incendios, nos entregarán paquetes, responderán a delitos, realizarán cirugía, ayudarán a la recuperación tras un desastre natural y proporcionarán compañía. La cifra de empresas noveles de robótica aumenta a una velocidad vertiginosa y hay quien calcula que los robots industriales por sí solos podrían ser un mercado de 37 000 millones de dólares ya en 2018[2].

Los robots son ordenadores, sistemas automatizados capaces de sobrepasar el plano digital puramente bidimensional de sus antepasados para tocar, influir e interactuar con el mundo corpóreo que los rodea. La mayoría de ellos pueden controlarse a distancia a través de Internet y mediante aplicaciones para *smartphones*, lo cual representa que multitud de ellos forman parte de la Internet de las Cosas. Este hecho tiene repercusiones trascendentales. Tal como ha observado Joi Ito, director del Media Lab del MIT, vivimos en una época de convergencia, un tiempo «en el que bits del mundo digital se están fusionando con átomos del mundo físico»[3].

Los robots se están adentrando en nuestro espacio tridimensional, un espacio que compartirán con nosotros. Como todos los objetos conectados a la Internet de las Cosas, los robots pueden ser pirateados, si bien las consecuencias de ello podrían ser mucho más trascendentales. A lo largo de su breve historia, la ciberdelincuencia se ha ocultado tras pantallas informáticas, un problema bidimensional que podía afectar a tu bolsillo o a tu cuenta bancaria. Pero ya no. Como consecuencia de los avances en robótica, la ciberdelincuencia finalmente escapará de sus confines virtuales e irrumpirá en el espacio físico. Y no estamos en absoluto preparados para lo que se nos viene encima.

El complejo (robótico) militar-industrial

Durante décadas, los robots industriales han trabajado codo con codo con obreros humanos en almacenes y fábricas, pero los robots industriales modernos son maravillas de la ingeniería, capaces de levantar cientos de kilos y trasladar objetos repetidamente con una precisión de 0,15 milímetros, una proeza que ningún humano puede igualar. En un principio, estas máquinas eran caras, con precios que rondaban varios cientos de miles de dólares, y requerían meses de programación informática altamente personalizada antes de poder realizar las tareas que se les asignaban. Pese a los costes, ningún sector se ha beneficiado más de la robótica que los fabricantes automovilísticos, que representaban el 40 por ciento de las ventas robóticas mundiales en 2013[4]. Los robots no sólo agilizan la producción de vehículos, sino que la hacen más segura, barata y eficiente, y todos los grandes fabricantes, desde Ford hasta BMW, los utilizan para automatizar la producción. En sólo una fábrica de Hyundai en Alabama, quinientos robots trabajan sin descanso soldando, pintando, atornillando y transportando piezas de automóviles para poder producir en serie más de mil coches al día[5]. Para no ser menos, Amazon anunció en 2014 que emplea diez mil robots Kiva Systems para recorrer sus inmensos almacenes en busca de artículos individuales y transportarlos a los empleados humanos que los empaquetan antes de entregárselos a otros robots para que procedan a su envío. Estos robots trabajan tres turnos al día, 365 días al año y no hacen pausa para el café[6].

El precio de los robots industriales se abarata exponencialmente, a la par que las máquinas se vuelven más eficientes y más fáciles de usar. Quizá el robot que mejor ejemplifique esta tendencia sea Baxter, el bot industrial de bajo precio tan mono creado por Rethink Robotics. Por sólo 22 000 dólares, cuesta una décima parte del precio de sus predecesores. Y lo más impresionante es que funciona tal cual se saca de la caja y puede montarse y encenderse en sólo una hora, frente a los dieciocho meses que se precisaban para integrar las generaciones previas de robots industriales en una operación en fábrica[7]. Baxter aprende a realizar tareas sencillas, como «asir y colocar» objetos en una cadena de montaje, en sólo cinco minutos. Tiene un rostro adorable sobre su casco con visor y dos brazos sumamente hábiles, capaces de moverse en cualquier dirección para realizar la tarea asignada. No requiere programación especial y aprende utilizando su visión informática para observar a un empleado realizar una tarea, que el robot puede luego repetir *ad infinitum*. Conforme estos costes vayan menguando, estos robots tendrán un precio competitivo en comparación con la mano de obra barata deslocalizada y muchos esperan que un auge en la robótica nacional propicie un renacimiento de la fabricación en Estados Unidos.

Actualmente hay robots en todas partes, desde restaurantes hasta hospitales. En más de 150 centros médicos es posible llamar a robots TUG de Aethon mediante una aplicación para teléfono inteligente con el fin de que recorran de manera anónima los pasillos para suministrar medicamentos, llevar la comida a los pacientes y encargarse de la colada, tareas que en el pasado realizaban los camilleros y camilleras[8]. Otros robots médicos, como el robot Da Vinci de Intuitive Surgical, permiten a los

cirujanos operar a pacientes mediante brazos robóticos. Equipados con un visor y controles de *joystick*, los médicos ven una imagen en 3D del interior del paciente y manipulan instrumental quirúrgico pequeño para practicar intervenciones que van desde histerectomías hasta reparaciones de válvulas cardíacas. Eliminada la necesidad de introducir grandes manos humanas en el cuerpo del paciente, la cirugía robótica puede realizarse con una invasión mínima, con un 80 por ciento menos de complicaciones e importantes reducciones en los tiempos de convalecencia. Cada año se realizan más de 500 000 operaciones de este tipo en todo el mundo[9]. Empleando una tecnología similar, un cirujano puede operar remotamente a un paciente a través de Internet mediante telecirugía similar; la primera intervención de este tipo tuvo lugar en 2001: desde Nueva York, un cirujano realizó una colecistectomía en el otro lado del Atlántico a una mujer de Estrasburgo, Francia[10].

Pese a que los logros de la robótica industrial y médica han sido impresionantes, el desarrollo de la robótica militar ha sido asombroso[11]. En 2003, el Pentágono tenía menos de 50 VANT en su arsenal[12]. Actualmente, Estados Unidos posee una cifra de robots superior a la de ningún otro país, «con unos 11 000 drones y 12 000 robots terrestres desplegados en todo el mundo»[13]. Estas máquinas van bien armadas y son letales, fe de lo cual da que hayan abatido ya a miles de personas[14]. Se calcula que, en 2011, uno de cada cincuenta soldados destacados en Afganistán era un robot y que, en 2023, habrá diez robots por soldado humano en el Ejército estadounidense[15].

Los vehículos terrestres no tripulados (UGV), como el PackBot de iRobot, participan de manera rutinaria en la detección y eliminación de dispositivos explosivos improvisados (DEI). El TALON de Foster-Miller es un «robot portátil que opera en caminos estrechos», como un tanque en miniatura. Puede equiparse con metralletas, rifles del calibre .50, lanzagranadas y cohetes antitanque, todo ello mientras se controla a distancia mediante un *joystick*. El Sand Flea de Boston Dynamics sólo pesa cinco kilos, pero es capaz de saltar hasta nueve metros de alto y aterrizar en la azotea de un edificio o saltar con precisión a través de una ventana abierta, a la par que capta todo lo que ve con su cámara de alta definición. La empresa también ha creado a BigDog, un robot de cuatro patas capaz de transportar hasta 180 kilos de equipamiento y armas, caminar con facilidad por terreno accidentado y acatar obedientemente la voz del soldado que lo controla[16]. Otros UGV como RiSE, una cucaracha robótica de seis patas, son capaces de trepar muros, el Cheetah corre 50 kilómetros por hora (más que Usain Bolt), BEAR es capaz de rescatar a un soldado herido del campo de batalla y un robot del tamaño de un maletín de la marca iRobot emplea el reconocimiento facial para identificar a un hombre entre una multitud y seguirlo[17].

En los cielos, las aeronaves sin piloto o VANT, recopilan imágenes, interceptan comunicaciones y lanzan misiles contra sus objetivos. Pilotos remotos sentados en la otra punta del mundo pueden matar a enemigos (y, en ocasiones, a inocentes) con un

clic de ratón[18]. Según Peter Singer, un destacado experto en robótica militar, al menos otros cincuenta y cinco países poseen programas de robótica militar. Los drones se han convertido en un elemento central del arsenal militar y se prevé que «el gasto mundial en drones, tanto militares como civiles, alcance acumulativamente los 89 000 millones de dólares» en 2023[19]. Hay drones grandes, drones pequeños, drones helicóptero, drones de mano e drones insecto. Los VANT como el MQ-9 Reaper cuestan en torno a 12 millones de dólares, una décima parte del precio de un caza F-22, y presentan prácticamente las mismas funcionalidades[20]. Los oficiales del Ejército destacan que los drones como el Reaper y el Predator están diseñados para llevar a cabo la llamada *kill chain* («cadena de muertes») íntegra contra sus objetivos de gran valor: «localizarlos, fijarlos, seguirlos, apuntar, ejecutar y evaluar» los daños.

El Leviatán de la flota de drones es el Global Hawk. Con una envergadura de 40 metros en las alas y un peso de 14 500 kilogramos, puede aerotransportarse durante cerca de dos días a una altitud de 60 000 pies. Los sensores de la flota de VANT son igualmente impresionantes e incluyen herramientas como la ARGUS-IS, la cámara de máxima resolución del mundo, capaz de tomar fotografías de 1,8 gigapíxeles. La ARGUS está equipada con una capacidad de «mirada constante» equivalente a la de cien drones Predator, lo cual le permite rastrear todos los movimientos en tierra que se desarrollan dentro del perímetro de una ciudad mediana. Las imágenes son de tanta calidad que los drones pueden generar un millón de terabytes de datos al día, el equivalente a cinco mil horas de metraje en alta definición, registran hasta el último movimiento en tierra (coches, autobuses, personas y perros) y pueden reproducirse rebobinando o avanzando hacia delante a voluntad, como cualquier vídeo grabado[21].

Un aspecto importante es que los drones hace tiempo que han abandonado el ámbito exclusivo de la guerra y ahora realizan vuelos nacionales sobre Estados Unidos del continente en misiones como vigilancia de narcotraficantes, delincuencia organizada y cruce de fronteras por parte de inmigrantes ilegales. Los contratistas militares tradicionales como Northrop Grumman, Boeing y Lockheed Martin fueron de los primeros en apuntarse al campo de la robótica, seguidos por empresas especializadas de menor tamaño, como Boston Dynamics e iRobot (en efecto, la misma casa que fabrica el aspirador Roomba es artífice del PackBot de eliminación de dispositivos explosivos improvisados). Ahora bien, se ha producido otra incorporación profundamente perturbadora al mundo de la robótica: Google.

El gigante de las búsquedas se ha dispuesto a adquirir robótica y ya ha comprado ocho empresas de robótica distintas en un período de seis meses en 2014, incluidas entre ellas empresas especializadas en robots humanoides que caminan, brazos robóticos, *software* robótico y visión artificial[22]. Ahora bien, su adquisición robótica de mayores dimensiones y más sorprendente fue la empresa de robótica militar Boston Dynamics, los mismos tipos que fabrican el BigDog, el Cheetah, el Sand Flea, el RiSE y el PETMAN (un robot humanoide bípedo que bien podría ser el soldado

del futuro). Asimismo, Google superó la oferta de Facebook para la adquisición de Titan Aerospace, un fabricante de drones del tamaño de cazas que funcionan con energía solar y pueden permanecer en vuelo durante tres años sin aterrizar. ¿Por qué compiten dos gigantes de la Red por la superioridad aérea? Afirman que los drones pueden utilizarse para proporcionar acceso a Internet a regiones del mundo que aún no están en línea. Sin embargo, cuando una de las empresas de inteligencia artificial y datos más importantes del mundo se interna en el ámbito de la robótica y deviene capaz de lanzar sus propios ejércitos de drones, es preciso plantearse bien cuáles son sus intenciones y capacidades.

Un robot en cada hogar y en cada oficina

Para los robots, el salón de tu casa es la última frontera.

CYNTHIA BREAZEAL, Media Lab del MIT

En un artículo imprescindible publicado en *Scientific American*, Bill Gates comparaba los robots industriales con las macrocomputadoras y predecía que la miniaturización, los estándares técnicos comunes y unos mejores sensores acabarían por llevar un robot a cada hogar en el futuro próximo[23]. Y todo apunta a que tenía razón[24]. Ya existen robots domésticos que limpian suelos, riegan las plantas, limpian las barbacoas y alimentan a las mascotas. iRobot ha vendido más de diez millones de sus aspiradores Roomba desde su lanzamiento y pueden encontrarse en cualquier tienda de electrodomésticos o Walmart local. Los niños cada vez juegan con más juguetes robóticos, como los Mindstorms de Lego, Robosapien X de WowWee y la Robotic Ball de Sphero. Incluso la excepcional ama de casa Martha Stewart ha adquirido un dron *cuadricóptero* (o cuadrirrotor) DJI Phantom con una cámara HD, que disfruta teledirigiendo por su inmensa finca de 61 hectáreas en Nueva York[*] [25]. El mercado de robots para el consumo y de oficina se está disparando por los aires, con un crecimiento siete veces más rápido que la demanda de robots industriales[26].

Hasta ahora, la mayoría de los robots domésticos se han diseñado para realizar una sola tarea, como por ejemplo pasar el aspirador. Sin embargo, en el futuro dispondremos de robots multifuncionales capaces de realizar muchas otras cosas, como recoger la mesa después de las comidas, poner el lavavajillas, planchar nuestras camisas y recoger los juguetes de los niños, todo ello fácilmente controlado desde la familiar pantalla de nuestros teléfonos inteligentes. Y aunque estos ayudantes del hogar de ensueño aún tienen que materializarse y pueden tardar años en hacerlo, se están realizando progresos. Una campaña de micromecenazgo en Indiegogo dirigida por Cynthia Breazeal del MIT recaudó fondos para crear un útil e inteligente robot

social llamado Jibo, capaz de identificar a los miembros individuales de un hogar, tomar fotografías familiares, leer correos electrónicos, contar cuentos a los niños a la hora de dormir y modificar la expresión facial para mostrar emociones. El PR2 de Willow Garage ya es capaz de plegar la ropa, sacar una cerveza de la nevera, recoger las deposiciones del perro, hornear galletas y cocinar un desayuno completo[27]. Tanto en Japón como en Europa y Estados Unidos, la cantidad de fondos invertidos en investigación y desarrollo de robótica no tiene precedentes.

Es cierto que algunos de estos avances parecen salidos de una novela de Philip K. Dick. Por ejemplo, en Corea del Sur y en Japón ya existen robots niñera. Juegan con los niños y pueden mantener conversaciones limitadas con reconocimiento de voz. Muchos de ellos utilizan los ojos robóticos para transmitir en directo vídeo de tus hijos a tu ordenador o teléfono inteligente. El robot niñera PaPeRo de NEC te permite además hablar con tus hijos directamente o enviarles mensajes de texto, que el robot les lee, y el robot Pepper de SoftBank proclama «ser capaz de interpretar las emociones y expresiones faciales de tu hijo y reaccionar de manera adecuada»[28]. Pese a que los robots niñera pueden ser de utilidad para los padres agotados por el trabajo y con sueño atrasado de todo el mundo, otro campo de la robótica personal que registra una expansión aún más acelerada es el de los robots para el cuidado de ancianos. Habida cuenta de las tendencias demográficas y del envejecimiento de la población en los países desarrollados del mundo, hay escasez de cuidadores que proporcionen a las personas de la tercera edad los cuidados emocionales y físicos que requieren. Este desafío es principalmente importante en Japón, donde cerca del 25 por ciento de la población supera los sesenta y cinco años. Para aliviar este problema, el gobierno del primer ministro Shinz Abe destinó 2390 millones de yenes en 2013 a contribuir al desarrollo de robots para el cuidado de ancianos a nivel nacional[29]. Un ejemplo de este tipo de robots es Paro, un adorable robot con forma de cría de foca arpa que hace compañía a los ancianos. Paro «es capaz de reconocer voces individuales, rastrear movimientos y recordar comportamientos que despiertan respuestas positivas en los pacientes». Cuando se lo acaricia, responde arrullando y acurrucándose a la persona que lo toca. Ya se han vendido millones de ejemplares Paro en todo el mundo y han demostrado ser especialmente útiles en pacientes con demencia avanzada, en quienes han reducido los niveles de agresividad y han mejorado el humor[30]. Consciente de la demanda de robots para el cuidado de ancianos, iRobot, fabricante de aspiradores y robots asesinos, ha abierto una nueva división específica para satisfacer las necesidades de la tercera edad.

Una de las clases de robots para el cuidado de ancianos que crece a mayor ritmo son los robots de telepresencia, máquinas que permiten a las personas «desplazarse virtualmente por un edificio en la distancia mediante el control remoto de un robot con ruedas equipado con una cámara, un micrófono, un altavoz y una pantalla que muestra vídeo en directo» del rostro de la persona que controla el robot a través de Internet[31]. Robots como el MantaroBot y el GiraffPlus de la UE permiten a los hijos

«iluminar con su presencia» la estancia e interactuar con sus padres envejecidos desde kilómetros de distancia mediante un robot con ruedas y un rostro parecido a un iPad controlado de manera remota[32]. De este modo, se puede comprobar cómo se encuentran los parientes viejecitos, compartir comidas con ellos a través de conversaciones de vídeo al estilo de Skype e incluso asegurarse de que se han despertado y no se han caído en sus hogares. Ahora bien, no sólo los adultos preocupados utilizan los *bots* de telepresencia para comprobar cómo están sus progenitores, sino que éstos se emplean cada vez más también en hospitales. El RP-VITA (siglas de Remote Presence Virtual + Independent Telemedicine Assistant o «asistente de telemedicina independiente con presencia virtual remota») de iRobot permite a los médicos, en particular a los especialistas, aparecer junto a las camas de sus pacientes y diagnosticarlos sin necesidad de hallarse físicamente en la misma habitación. Con sólo pulsar un botón en el iPad, un doctor desde la otra punta de la ciudad o del mundo puede dirigir al robot junto a la cama del paciente, ampliar la imagen de sus pupilas e incluso solicitarle a una enfermera que le coloque un estetoscopio en el pecho para auscultarlo desde la distancia y determinar su frecuencia cardíaca[33]. El tiempo nos dirá si los robots serán más agradables con los enfermos que los humanos.

También el sector empresarial empieza a cobrar conciencia del valor de contar con robots de telepresencia en la oficina, los cuales permiten a sus empleados ausentarse físicamente mediante dispositivos controlados a distancia. Empresas como Suitable Technologies y Double Robotics disponen de modelos que cuestan en torno a 3000 dólares y permiten a sus empleados trabajar desde casa mientras sus alter egos robóticos deambulan por los pasillos de la oficina, se acercan a los escritorios de sus colegas o se ponen al tanto de los últimos cotilleos a la hora de la comida. Incluso el famoso filtrador de la NSA Edward Snowden utilizó un *bot* de telepresencia para hacer una presentación frente a un público de miles de personas en las conferencias TED celebradas en 2014 en Vancouver, sin tener que preocuparse por abandonar su refugio secreto y seguro en Rusia.

No se admiten candidatos humanos

Con el transcurso del tiempo veremos cómo aparecen robots capaces de realizar cualquier tarea o empleo. La cadena de hoteles Starwood ya ha incorporado mayordomos robóticos, «en servicio día y noche»[34]. Estos robots son capaces de desplazarse hasta la habitación de cualquier huésped y llevarle el cepillo de dientes que ha olvidado o llevarle el servicio de habitaciones que ha solicitado, lo cual deja espacio libre al personal para ocuparse de otras tareas. El robot fabricante de

hamburguesas de Momentum Machines es capaz de satisfacer pedidos de hasta 360 hamburguesas en su punto por hora, cada una de ellas con los ingredientes adicionales (lechuga, *ketchup*, cebollas…) solicitados por los clientes.

Un estudio de 2013 realizado por la Oxford University acerca del futuro del trabajo analizó en detalle más de setecientas profesiones y concluyó que el 47 por ciento de los trabajadores estadounidenses corren el riesgo de perder sus trabajos a consecuencia de la automatización robótica en un horizonte tan temprano como 2023[35]. Quienes trabajan en el sector de los transportes (taxistas, conductores de autobús, camioneros de larga distancia, conductores de FedEx y repartidores de *pizza*) afrontan un riesgo especial, pues la probabilidad de que sus empleos se sustituyan por vehículos autónomos asciende a un 90 por ciento. Ahora bien, no sólo los empleos de perfil más bajo están en riesgo[36]. Agencias de prensa como Associated Press y *Los Angeles Times* utilizan robots y algoritmos para escribir automáticamente miles de artículos sobre temas tan diversos como homicidios, seísmos y los últimos beneficios empresariales[37]. «El *software* de procesamiento de imágenes es capaz de analizar las biopsias con más precisión que los técnicos de laboratorio», y QuickBooks es capaz de gestionar la mayoría de las tareas que realiza un contable. Muchos creen que el aumento de la automatización y la robótica es lo que ha comportado el profundo estancamiento salarial registrado desde 2004[38]. Bill Gates fue clarividente en sus predicciones acerca del futuro de la robótica y la presencia de un robot en cada hogar y oficina. No obstante, ya trabajes volteando hamburguesas, conduciendo un camión o redactando noticias de última hora, cualquiera que haya leído *Las uvas de la ira* de John Steinbeck sabe que las transiciones industriales son brutales para quienes quedan relegados.

Es posible que incluso la deslocalización sea reemplazada por la externalización robótica, eliminando aún más empleos de seres humanos tanto en territorio nacional como en el extranjero. A medida que las máquinas ganen en inteligencia y se vuelvan más capaces, la raza humana podría experimentar un renacimiento increíble en el que todas nuestras tareas diarias las desempeñen robots y ello nos permita llevar una vida ociosa, con tiempo libre ilimitado para cantar, bailar y pintar mientras bronceamos nuestros músculos atrofiados en cualquier playa. O podría pasar lo contrario: que la sociedad degenerar en un caos a medida que masas de desempleados y personas que jamás podrán incorporarse a la población activa se revolucionen contra los pocos zares humanos que controlen los robots del mundo. La balanza podría inclinarse en una u otra dirección, dependiendo de las decisiones que adoptemos hoy en materia de política pública, legislación, economía y ética.

Los derechos de los robots: legislación, ética y privacidad

Un hombre sin ética es una bestia salvaje soltada en este mundo.

ALBERT CAMUS

Si bien nadie defendería que tu Roomba debería quedar protegido por la Declaración Universal de Derechos Humanos de las Naciones Unidas, a medida que los robots se vuelvan más inteligentes y potencialmente conscientes en el futuro lejano, sin lugar a dudas estas cuestiones se pondrán sobre la mesa. En el ínterin, los robots de nuestro mundo plantean múltiples aspectos relativos a las políticas públicas, la legislación y temas éticos que exceden su impacto en la mano de obra. Si de manera accidental un cirujano robótico perfora una arteria y ocasiona la muerte al paciente, ¿puede la familia de la víctima demandar al robot o a su fabricante por mala praxis? Cuando un coche autopilotado se vea involucrado en un accidente, ¿de quién será la culpa? ¿Podrá demandarse al pasajero que no lo conducía? ¿A la empresa fabricante del vehículo, tal vez? ¿O tal vez a la empresa que programó el *software* de conducción y navegación? Cuando esté claro que un vehículo autónomo está a punto de verse implicado en una colisión inevitable, ¿debería el algoritmo de optimización antichoque determinar si es mejor que colisione contra el poste telefónico (lo cual comportaría la muerte del pasajero), contra el motorista de la izquierda, contra el Chevrolet de la derecha o contra el peatón que pasa por delante? Pese a que nuestra capacidad de construir y desplegar robots avanza exponencialmente de manera acelerada, en términos éticos aún nos hallamos en la más tierna infancia.

Si bien la existencia ubicua de robots se perfila en el horizonte, escasean los defensores de la ética robótica, expertos políticos y legisladores capaces de dar respuesta a los complejos interrogantes que los avances científicos plantearán a la humanidad. En concreto, seremos testigos de nuevos ataques a la privacidad hasta ahora inconcebibles. Al igual que las redes sociales, aplicaciones y teléfonos móviles antes que ellos, los robots se suministrarán con términos de servicio que detallarán las condiciones que protegerán a los fabricantes de robots y afectarán a tu privacidad. Pese a que ahora tu robot aspirador, tu *bot* para el cuidado de ancianos o tu juguete robótico permanezcan sentaditos en un rincón con aspecto inocente y tierno, listos para complacerte en el preciso instante en que se lo solicites, lo cierto es que están equipados con una serie de cámaras, micrófonos y sensores capaces de ver y grabar todo lo que haces en la privacidad de tu hogar.

Los drones recreativos equipados con cámaras de alta definición ya están planteando amenazas a la privacidad previamente desconocidas. A mediados de 2014, una joven de Seattle que vivía en la vigesimosexta planta de un bloque de viviendas se sorprendió al ver a un *cuadricóptero* (un pequeño robot con cuatro rotores)

planeando al otro lado de su ventana filmándola mientras se cambiaba en su dormitorio: un robot «mirón» del siglo XXI[39]. En otro incidente acontecido en Seattle, un hombre decidió hacer volar su dron personal equipado con cámara sobre el patio trasero de un vecino. Cuando la vecina escuchó el ruido, que atribuyó a que alguien estaba utilizando una desbrozadora en su jardín, abrió las cortinas de su dormitorio, situado en la segunda planta, para investigar y encontró a un dron merodeando al otro lado de su ventana, a uno o dos metros de distancia. Envió a su marido a averiguar qué ocurría y éste descubrió a un vecino teledirigiendo el avión; ante la solicitud de que dejara de filmar automáticamente, el piloto del robot invasor respondió con una negativa, argumentando que era legal hacerlo. Quizá tuviera razón.

Mientras que pisar el jardín de otra persona se considera allanamiento de morada, no ocurre lo mismo al sobrevolarlo con un helicóptero (sea grande o pequeño), como resultado de una decisión adoptada por el Tribunal Supremo en 1946 que establecía que: «El aire es una autopista pública»[40]. Por supuesto, los policías de Seattle que acudieron a la escena de aquellos incidentes se mostraron confusos, y no son los únicos. De acuerdo con un informe gubernamental de 2012 sobre drones privados que vuelan por Estados Unidos, la Oficina de Responsabilidad Gubernamental (GAO en sus siglas en inglés) concluyó que: «Actualmente, ningún organismo federal posee una responsabilidad legal específica para regular asuntos de privacidad relativos a los sistemas de aeronaves no tripuladas para el gobierno federal en su globalidad. Dada la capacidad de estos dispositivos de albergar cámaras de alta definición, sensores infrarrojos, tecnología de reconocimiento facial y lectores de matrículas, hay quien argumenta que los drones presentan un riesgo para la privacidad sustancial»[41]. ¿Tú qué opinas?

Interrogarse acerca de quién posee los derechos aéreos por encima de las propiedades y quién puede ser filmado dónde es sólo el principio de un conjunto hondamente complejo de aspectos legales, éticos y de políticas públicas que sin duda aflorarán con mucha mayor frecuencia a medida que el uso de robots prolifere en nuestra sociedad. Podría considerarse que quien planteó inicialmente estas cuestiones fundacionales, ya en 1942, fue Isaac Asimov, con la publicación de su relato breve «Círculo vicioso», en el que acuñó el término «robótica» y expuso sus famosas Tres leyes de la robótica:

1.ª Un robot no hará daño a un ser humano o, por inacción, permitirá que un ser humano sufra daño.
2.ª Un robot debe obedecer las órdenes dadas por los seres humanos, excepto si estas órdenes entrasen en conflicto con la primera Ley.
3.ª Un robot debe proteger su propia existencia en la medida en que esta protección no entre en conflicto con las leyes Primera o Segunda.

Pese a que Asimov nos brinda un excelente punto de partida a partir del cual plantearnos estos aspectos, a estas alturas aún no somos capaces de programar una máquina para que entienda concretamente el concepto de «desayunar», por no hablar

ya de un idea tan abstracta como el «daño». Probablemente los robots requerirían un código ético mucho más flexible y adaptable, código que no estamos ni siquiera lejos de construir por ahora. Pese a ello, avanzamos imparables hacia la robótica industrial, militar, médica y personal generalizada, y es inevitable que ocurran accidentes.

Peligro, Will Robinson

«¡Peligro, Will Robinson!» era la frase que repetía con frecuencia el robot que protegía al joven aventurero espacial para advertirle de amenazas inminentes en la serie televisiva de la década de 1960 *Perdidos en el espacio*. Ojalá todos los robots tomaran tales precauciones en sus interacciones con los seres humanos. A medida que las personas interactuemos más con los robots, se producirán consecuencias imprevistas, como podrían ser lesiones graves o incluso la muerte a manos de las máquinas, incluso de aquellas concebidas para ayudarnos. En 2013, la Food and Drug Administration (FDA) inició una investigación en torno a numerosos accidentes de daños provocados por el robot médico Da Vinci de Intuitive Surgical, incidentes que, al parecer, la empresa no había comunicado al gobierno, tal como exige la ley[42]. En un caso, a un hombre le perforaron el colon durante una cirugía de la próstata. En otro, el robot agarró el tejido abdominal del paciente durante una cirugía colorrectal y se negaba a soltarlo pese a los esfuerzos del cirujano humano por abrir las garras de la mano mecánica; fue preciso reiniciar el Da Vinci para que finalmente soltara el tejido de aquel hombre. En un tercer caso, un robot quirúrgico golpeó en la cara a una mujer mientras le practicaban una histerectomía[43].

La abrumadora mayoría de las lesiones consecuencia de la interacción entre humanos y robots están provocadas no por robots quirúrgicos, sino industriales. A pesar de la inexistencia de estadísticas completas en cuanto a accidentes robóticos a escala mundial, son numerosos los informes acerca de tales accidentes. En 2007, por ejemplo, un obrero de Estocolmo que creía haber apagado un robot se acercó a la máquina para repararla. Por desgracia, el robot seguía estando encendido, se activó, agarró al hombre con fuerza por la cabeza, lo levantó del suelo y le rompió cuatro costillas antes de que el pobre hombre pudiera desembarazarse de él[44]. En cualquier colisión entre un hombre y una máquina, es probable que la máquina gane, y en muchos casos el resultado ha sido una muerte. Uno de los primeros casos de homicidio robótico ocurrió en 1981, cuando un empleado de treinta y siete años de Kawasaki Heavy Industries llamado Kenji Urada se dispuso a reparar un robot que no había desconectado por completo. Al estar fuera de su campo de visión, el potente brazo hidráulico del robot golpeó de forma accidental al hombre, que fue a caer en una rectificadora cercana, donde murió aplastado. En Estados Unidos, un empleado

de una fábrica automovilística murió en 2001 al acceder a la carcasa desbloqueada del robot para limpiarla. La máquina confundió al obrero con una pieza de coche, lo agarró por el cuello y lo retuvo colgado hasta asfixiarlo. De acuerdo con la Administración de Seguridad y Salud Ocupacional, sólo en Estados Unidos se han producido al menos treinta y tres muertes, cifra que probablemente aumente a medida que los robots salgan de sus jaulas y empiecen a caminar entre nosotros[45]. Según parece, no todos los robots conocen al señor Asimov y sus tres leyes.

Los accidentes robóticos se volvieron mucho más graves cuando se decidió que era buena idea dotar a los robots de armas completamente automáticas, tal como descubrieron los miembros de la Fuerza de Defensa Nacional de Sudáfrica en 2009 durante un ejercicio de entrenamiento con munición de verdad. El arma antiaérea de doble cañón de un Oerlikon MK5 controlado informáticamente registró un aparente error de *software*, por el que el dispositivo disparó en modo plenamente automático a una velocidad de 550 proyectiles por minuto mientras describía salvajemente círculos completos como un aspersor descontrolado en un jardín. Al final, nueve soldados resultaron muertos, incluidas varias mujeres, y otros catorce quedaron gravemente heridos, en una escena salpicada de sangre reminiscente de una película de *Terminator*[46]. Este incidente demuestra que cuando un robot encuentra una «pantalla azul de muerte» informática, puede provocar muertes reales y tener una repercusión trascendental en nuestro espacio físico tridimensional común. Y no sólo fallan los robots industriales o terrestres, sino también los voladores.

Según un artículo aparecido en el *Washington Post*, más de cuatrocientos VANT del Ejército han caído de manera accidental del cielo, tanto en el interior del país como en el extranjero, y han «impactado contra viviendas, granjas, carreteras, autopistas y, en un caso, un avión cargo C-130 Hercules de las Fuerzas Aéreas en pleno vuelo»[47]. No hay que lamentar víctimas mortales en estos accidentes, por esto sólo puede atribuirse a un milagro.

En 2009, el piloto de un dron perdió el control de un VANT Reaper armado con una envergadura de veinte metros que se adentró volando descontrolado en Afganistán. Para detener a aquel robot volador renegado hubo que enviar dos cazas estadounidenses que lo derribaron antes de que entrara en el espacio aéreo de Tayikistán.

En Estados Unidos, cerca de cincuenta drones se han estrellado, incluida una aeronave no tripulada del Ejército de 170 kilos de peso que se estrelló contra el suelo cerca de una escuela primaria de Pensilvania, «justo minutos después de que los alumnos se hubieran marchado a casa»[48]. Los accidentes robóticos son la excepción y ocurren con muy escasa frecuencia y, además, se están adoptando medidas activas para dotar a los robots de sistemas de detección y evitación de colisiones para impedir muchos de los accidentes parecidos a los de los robots industriales. Pese a ello, dado el tremendo auge que se prevé que registren tanto los robots domésticos como los laborales, los robots de fábricas, los robots cirujanos y los robots bélicos, el

potencial de que se produzcan daños dista mucho de ser trivial, un riesgo que se incrementará de manera significativa cuando los robots se conecten a la Internet de las Cosas y agentes malintencionados puedan controlarlos ilegítimamente desde la distancia.

Robots pirateados

> En el futuro, cuando Microsoft deje un fallo de seguridad en su código, ello no implicará que alguien pueda colarse en tu ordenador, sino que implicará que alguien podrá asumir el control de tu robot criado y éste se dedicará a limar el filo de un cuchillo desde el umbral de la puerta de tu dormitorio mientras te observa dormir.
>
> DANIEL H. WILSON, roboticista y escritor

Existen docenas de sistemas operativos robóticos, la mayoría patentados, que gestionan desde sistemas armamentísticos militares hasta sistemas de control industrial SCADA. Ahora bien, al igual que los ordenadores de sobremesa y teléfonos móviles acabaron fusionándose en torno a unos cuantos sistemas operativos principales, lo mismo está sucediendo en el campo de la robótica con ROS (Robot Operating System). Esto tendrá una repercusión positiva enorme en el futuro de la robótica, pues los programadores no tendrán que reinventar la rueda cada vez que quieran codificar una función particular de un robot. ROS es gratuito y de código abierto y proporciona módulos para la simulación, el movimiento, la visión, la navegación, la percepción y el reconocimiento facial robóticos, entre otros muchos aspectos. Precisamente son esta clase de esfuerzos comunitarios de código abierto y la construcción de una experiencia compartida, apenas concebibles hace unos pocos años, los que permiten a empresas como Rethink Robotics comercializar el Baxter por 22 000 dólares en lugar de por 200 000.

ROS, desarrollado originalmente en Willow Garage en 2007, está financiado actualmente por la Open Source Robotics Foundation y se ejecuta en cualquier tipo de robots, desde pequeños juguetes hasta grandes máquinas industriales. Tal como se ha indicado varias veces a lo largo de este libro, no existe ningún ordenador que no pueda hackearse, una máxima que se aplica también a los robots, con implicaciones relevantes para la seguridad del conjunto de la población. De manera involuntaria, el hecho de que exista un sistema estandarizado, el Robot Operating System, facilitará la labor a los piratas informáticos, pues les proporcionará un objetivo unificado al cual atacar. La estandarización de un ROS universal allana el camino a ciberataques de mayor escala, tal como hemos visto que ocurrió con los ordenadores personales. Y lo más importante, existe una diferencia abismal entre piratear robots y piratear otros sistemas informáticos y objetos de la Internet de las Cosas, y es que los robots se

desplazarán por nuestro espacio físico, donde caminarán, conducirán, volarán y nadarán a nuestro alrededor. Los robots conectados a Internet pueden piratearse y redirigirse de diversos modos peligrosos y siniestros, hecho que delincuentes y terroristas no han pasado por alto. Cuando se subyugan robots, los *hackers* no sólo pueden utilizar los sensores de la máquina para espiar, sino que también pueden usar el motor de accionamiento robótico del dispositivo, sus brazos, piernas y ruedas para perseguir, golpear, patear, empujar, disparar, apuñalar, arrastrar y asesinar.

En esencia, los robots no son más que ordenadores en movimiento, ordenadores que liberarán a los ciberdelincuentes de las pantallas bidimensionales tras las cuales se ocultan hoy y los arrojarán a nuestro mundo físico cotidiano. Un equipo de investigación de la Universidad de Washington examinó tres robots domésticos, incluidos el Erector Spykee el Robosapien de WowWee y Rovio, y descubrió importantes fallos de seguridad en todos ellos, incluida la ausencia de contraseñas y una encriptación ausente o pobre[49]. Por tanto, terceras partes podían apoderarse de los dispositivos de manera remota, desplazarlos y capturar audio y vídeo. Los investigadores describieron la seguridad en estos dispositivos como una «mera consideración tardía». No obstante, a medida que los robots cobren más presencia en la sociedad y habiten nuestro mundo, se unirán a los miles de millones de objetos adicionales conectados a la Internet de las Cosas. Tal como hemos visto previamente, decenas de miles de sistemas de videoconferencias utilizados en despachos de abogados, empresas farmacéuticas y centros médicos son profundamente inseguros y se han vulnerado con éxito, incluso en la sala de juntas de Goldman Sachs. ¿Por qué iban a ser diferentes los *bots* de telepresencia, que no son más que dispositivos de videoconferencia móviles? Estos robots podrían perseguirte y escucharte a hurtadillas o bien permanecer sentados en silencio durante las reuniones observándolo todo, lo cual los convertiría en magníficas herramientas para el espionaje industrial. Y cuando una fábrica cierre al final del día y se apaguen las luces, piratas informáticos desde la otra punta del mundo podrían apoderarse de los robots para reconocer el terreno antes de atacar. Y aunque haya un guarda de seguridad para evitar que se cuelen delincuentes, también es posible que uno de esos delincuentes sea un robot y ya esté dentro del edificio.

La piratería de robots plantea una serie de preguntas importantes. ¿Qué grado de privacidad tiene esa consulta clínica robótica que tu médico te está realizando a través de Internet? Peor aún, esos robots industriales que cocinan hamburguesas y trocean tomates estarán armados con cuchillos afilados, pero… ¿cómo podemos enseñarles a que tengan cuidado cuando hay humanos cerca? Pese a que la mayoría de los robots industriales incorporan sistemas de seguridad, tal como hemos visto, se producen accidentes, algunos de ellos letales. Además, las rutinas de seguridad robóticas están codificadas en programación informática, programación que los *hackers* pueden manipular y desactivar. Las próximas generaciones de robots domésticos potentes podrían utilizarse indebidamente de modos que los diseñadores no habían previsto.

Del mismo modo que los usuarios de teléfonos inteligentes liberan sus iPhone hoy en día para eliminar las restricciones al *software*, es posible que hagan lo propio con sus robots y abran la puerta a una amplia variedad de situaciones en las que los «robots se descontrolan».

Imagina por ejemplo un ataque típico de «en la pantalla confiamos» en el que un empleado apaga el robot antes de limpiarlo, como debe hacerse, pero un *hacker* lo ha manipulado para que permanezca encendido. Pese a que la pantalla muestra que el robot y sus gigantescos brazos industriales están desconectados, al acercarse a la máquina el inocente trabajador podría ser agarrado por el cuello, levantado en el aire y morir asfixiado, un modo fantástico de acabar con ese compañero del sector 3B que nunca te cayó bien. A ojos del mundo, se antojaría otro accidente más. Y si estas situaciones te parecen inverosímiles, has de saber que ya existen casos demostrados de vulneración de algunos de los robots más seguros del mundo (militares y policiales).

Juego de drones

> Hay que controlar los drones. Hay de establecer algunas reglas de uso para evitar o minimizar las bajas colaterales. Es sumamente importante.
>
> VLADIMIR PUTIN

A finales de 2009, mientras las guerra escalaba en Oriente Próximo, drones estadounidenses Predator surcaban de manera casi constante los cielos de Irak. Sus misiones englobaban desde la recopilación de imágenes de espionaje hasta «operaciones cinéticas contra objetivos de gran valor», como lanzar misiles Hellfire contra los insurgentes. Los pilotos de los drones encargados de cubrir estas operaciones desde el desierto de Nevada, a 11 000 kilómetros de distancia, observaban atentamente los canales de vídeo en directo de sus objetivos mientras perseguían a su presa con las aeronaves no tripuladas. Pero resulta que no eran los únicos que estaban observando. Militantes chiíes habían hallado un modo de subvertir la flota robótica voladora estadounidense y capturar sus retransmisiones de vídeo en directo[50]. Con un fragmento de *software* de piratería rusa con un precio de 26 dólares conocido como SkyGrabber, *software* que suele venderse en la clandestinidad digital para robar señales de televisión satélite, los insurgentes lograron interceptar el metraje de vídeo que enviaban los drones Predator clasificados. De este modo, mientras los estadounidenses observaban a los insurgentes, los insurgentes observaban a los estadounidenses, lo cual les proporcionaba una ventaja táctica y una información privilegiada vital sobre los objetivos de la coalición. Si los militantes veían que el vídeo enfocaba su vivienda,

sabían que había llegado el momento de pensar en mudarse a un lugar alternativo, y sin tardanza.

Y ésta dista mucho de ser la única ocasión en que se ha vulnerado con éxito un dron; de hecho, incluso ha sucedido en el propio territorio de Estados Unidos. El Departamento de Seguridad Nacional de Estados Unidos (DHS en sus siglas en inglés) utiliza una flota de estos VANT para proteger la frontera, pero, en 2012, descubrió que no eran ni de lejos tan seguros como se pensaba. Alumnos de la Universidad de Texas en Austin habían detectado un modo de subvertir los drones e intentaron informar de ello al DHS, que se negó a creerles y aseguró que las aeronaves no tripuladas «no podían piratearse»[51]. Tras meses de tira y afloja, finalmente convencieron a los funcionarios de participar en una demostración a cargo de los estudiantes, momento en el que las lumbreras universitarias se hicieron con el control del robot volador y empezaron a desviarlo marcadamente de su curso, para pasmo de los oficiales del DHS. Los estudiantes perpetraron su ataque manipulando con éxito el GPS del dron y modificando sus coordenadas, todo ello con *hardware* y *software* que habían construido en la escuela por menos de mil dólares. Su profesor, Todd Humphreys (el hombre responsable del pirateo del GPS del superyate *White Rose of Drachs* mencionado con anterioridad), recalcó astutamente tras el incidente del DHS: «Dentro de cinco o diez años habrá 30 000 drones volando por el espacio aéreo nacional […] Y cada uno de ellos podría ser un misil potencial utilizado en nuestra contra»[52].

Hay otras personas conscientes de ello, incluidos los iraníes, que aplicaron con éxito la misma técnica para sobrecargar la línea de comunicación de un dron RQ-170 estadounidense que sobrevolaba su país y lo obligaron a activar el modo de piloto automático. El dron actuó de acuerdo con su programación y regresó a la base en Afganistán, o eso creía él. En realidad, los iraníes lograron modificar las señales de GPS del VANT y enviaron directamente a aquel soldado robótico a las manos de los Cuerpos de la Guardia Revolucionaria Islámica[53]. La captura del dron y de su tecnología clasificada fue un importante golpe de inteligencia que se anotaron los iraníes y demostró una vez más que los días del pirateo de robots ya están aquí. Es más, no sólo es posible piratear los drones, sino también sus sistemas de mando y control. En 2011, un potente virus atacó la flota de drones estadounidense, infectó las cabinas de manto de los VANT Predator y Repeater y registró todas las teclas pulsadas por los pilotos de las aeronaves durante sus misiones de vuelo sobre Afganistán[54]. El origen de aquella incursión seguía siendo desconocido a finales de 2014 y la investigación de aquel incidente seguía en curso.

En 2013, el *hacker* en serie Samy Kamkar concibió un ataque (y lo publicó en línea para que otros pudieran aprovecharlo) que le permitía pilotar su propio dron aéreo para buscar a otros robots voladores en el cielo, vulnerarlos y convertirlos en un ejército *botnet* físico de aeronaves no tripuladas bajo su control. El *software*, bautizado como SkyJack, deja al descubierto las conexiones inalámbricas de los

smartphones que controlan los drones —como el modelo Parrot AR, enormemente popular, que suele venderse en Costco— y permite a los *hackers* apoderarse de los sistemas de cámara y control de vuelo del dron víctima[55]. Se han vendido más de 500 000 VANT Parrot y la técnica de Kamkar podría resultar útil para secuestrar otros drones, como los que sin duda entregarán mercancías por las ciudades en los años venideros, lo cual permitirá enviar paquetes y *pizzas* a direcciones erróneas en tiempo real. El futuro de la delincuencia domótica pinta prometedor para Crimen, S. A., que ya ha empezado a invertir recursos importantes en este tema.

Robots con mal comportamiento

En 1982, en las calles de la estilosa Beverly Hills, en California, la policía detuvo a un delincuente un tanto insólito: un robot DC-2 que estaba distribuyendo ilegalmente panfletos en el distrito financiero de la ciudad. Cuando los agentes se acercaron a aquel robot solitario de cuatro patas sobre ruedas, descubrieron una máquina con un monitor de CRT antiguo, un teclado a modo de pecho y una cabeza con forma de casco de astronauta. La policía exigió al misterioso operador del robot que se identificara, pero, en lugar de ello, recibieron una retahíla de insultos a través del altavoz incorporado del robot. Contrariados, los policías intentaron desmontar el robot y llevárselo bajo custodia; mientras lo hacía, el robot empezó a chillar a grito pelado a la multitud de curiosos que se había agolpado alrededor de la escena: «¡Socorro! ¡Socorro! Me quieren desmontar». Al final, el robot fue «arrestado» y una grúa lo transportó hasta la comisaría de policía. Unas cuantas horas después, Gene Beley, dueño del robot de 30 000 dólares y fundador de la Android Amusement Corporation, se personó ante la policía tirando de las orejas a sus dos hijos adolescentes. Los muchachos habían sacado el robot profesional «de juerga» sin permiso paterno. Pese a que la policía sopesó la posibilidad de citar a Beley por aquel incidente, finalmente optó por liberar al robot bajo fianza. Cuando, al regresar a su domicilio, Associated Press entrevistó a Beley, el hombre afirmó que se alegraba de tener al DC-2 de vuelta en casa y añadió: «Ha sido como si hubieran encarcelado a un miembro de la familia». Y, si bien pudo ser el primero, lo que es seguro es que el DC-2 no será el último robot detenido.

Con el tiempo, los robots se utilizarán para colaborar en robos bancarios, atracos en la calle e incluso secuestros. Los piratas informáticos ya han creado la R2B2 o Robotic Reconfigurable Button Basher («aporreadora de botones robótica reconfigurable»), una máquina capaz de probar contraseñas repetidas en teléfonos iPhone y Android bloqueados, robados o perdidos a una velocidad de un intento por segundo[56]. El robot pirata se construyó por menos de 50 dólares a partir de varios servomotores, una aguja de disco de plástico y una cámara web que «observa la

pantalla del teléfono para detectar si ha conseguido descifrar la contraseña» (incluso los delincuentes utilizarán robots para realizar tareas repetitivas o aburridas). Los robots también pueden convertirse en el mejor amigo de un delincuente, tal como descubrió la policía de Taiwán a mediados de 2014, cuando intentó arrestar a un conocido traficante de drogas armado que había protegido firmemente su domicilio con diversos robots de vigilancia que reproducían vídeo en directo con el fin de prevenirle de la presencia policial[57].

Tal como hemos visto al inicio de este capítulo, los terroristas también utilizan robots a modo de armas y no se limitan a VANT de comercio generalizado con cargas pequeñas[58]. Tanto en Irak como en Afganistán, los terroristas han recurrido a los llamados VBIED (dispositivos explosivos improvisados transportados por vehículos), conocidos popularmente como coches bomba, con el fin de destruir múltiples edificios y convertir en escombros vecindarios enteros, cargando algunos vehículos con hasta tres mil kilos de explosivos. Los VBIED son armas potentes y han destruido numerosos objetivos alrededor del mundo, incluidas las Torres Khobar en Arabia Saudí, los barracones de los *marines* estadounidenses en Beirut y el Edificio Federal Murrah en Oklahoma City.

En la actualidad, los terroristas empiezan a utilizar armas robóticas como reemplazo de los VBIED del pasado. En un vídeo descubierto en Internet, ingenieros tocados con pañuelos palestinos de Ansar al Islam aparecen alardeando de sus habilidades técnicas mientras, encorvados, sueldan placas de circuitos informáticos. En la escena siguiente de un clip de cuatro minutos de duración se ve una camioneta conduciendo a través del desierto con una metralleta automática montada en un trípode en el maletero. A medida que la cámara se aproxima, queda claro que el vehículo no lo conduce ningún conductor, sino que se opera mediante unos rudimentarios controles robóticos colocados sobre el volante y los pedales. Momentos más tarde, la metralleta dispara varias ráfagas, cuando el motor de accionamiento robótico controlado a distancia acciona el gatillo[59].

Con sistemas como éstos, los yihadistas no necesitan convertirse en mártires. Y pese a que quizá se pierdan las setenta y dos vírgenes prometidas, podrán volver a presentarse en la batalla otro día. El potencial de los vehículos autodirigidos para un uso indebido no ha pasado por alto a algunas personas de los cuerpos de seguridad; de hecho, el FBI publicó un informe interno donde recogía sus temores acerca de su uso futuro como armas mortales. Los agentes predijeron que estos transportes robóticos podían utilizarse a modo de VBIED preprogramados para atravesar de manera anónima una población y detonar en el objetivo previsto[60]. Los temores que siempre hemos albergado acerca de los robots asesinos, retratados en películas como *Westworld, almas de metal*, *Blade Runner*, *RoboCop*, *Terminator* y *Yo, robot*, desgraciadamente podrían hallarse en las fases iniciales de hacerse realidad.

El ataque de los drones

Los drones dan miedo. No se puede razonar con ellos.

MATT GROENING

Cuando Jeff Bezos, el director ejecutivo de Amazon.com, anunció a finales de 2013 que la «tienda de todo» mundial pronto utilizaría drones octocópteros para entregar paquetes a sus clientes, el mundo se puso en guardia y prestó atención. Desde luego, otras empresas se habían adelantado a Bezos, como los empresarios que lanzaron en TacoCopter y el Burrito Bomber, por no mencionar el hotel de Las Vegas que entrega champán junto a la piscina a sus huéspedes con drones, pero el anuncio de Bezos era distinto[61]. Amazon había perfeccionado su logística y el hecho de utilizar drones para realizar las entregas a sus clientes sin duda cambiaría las reglas del juego en el negocio. En otoño de 2014, Google empezó a entregar artículos a modo de prueba piloto mediante un pequeño avión monoplano de 1,5 metros de envergadura. Bautizado como Proyecto Ala, el dron de Google está capacitado para volar en un radio de 16 kilómetros de sus almacenes, y entrega cualquier cosa, desde caramelos hasta comida para perros[62]. El VANT también incorpora robots y es capaz de planear a cien pies sobre la casa del cliente y descender los productos al suelo mediante un torno de cable antes de regresar a las oficinas de la empresa. Sin duda, estos servicios plantean muchos problemas, tanto técnicos como legislativos, pero, de una forma u otra, así es como está la situación: nos guste o no, la era de los drones comerciales y civiles ya está aquí.

Pese a que habitualmente se asocian con el Ejército y la guerra, los drones pueden ser una fuerza positiva. Se utilizan drones para detectar a cazadores furtivos en África y para ayudar a los agricultores a mantener sus cosechas en Estados Unidos. Fueron drones los que revisaron los daños en las instalaciones de Fukushima tras la fuga nuclear y también se usaron para ayudar tras el terremoto de Haití. En la actualidad, los VANT persiguen a las tormentas para proporcionar advertencias tempranas acerca de huracanes, apagar incendios forestales y transportar medicinas a poblaciones remotas. Los agentes inmobiliarios los emplean para fotografiar propiedades y padres como Paul Wallich de Vermont pilotan cuadricópteros sobre sus hijos durante el trayecto hasta el autobús de la escuela para asegurarse de que lleguen sanos y salvos[63]. La Policía Montada Real canadiense incluso ha utilizado sus roboguardias cuadricópteros en el primer caso de la historia de una vida salvada gracias a un VANT. Sobrevolaron con la aeronave una zona aislada de Saskatchewan para localizar a un hombre herido y desaparecido que se perdió y desorientó después de sufrir un accidente de tráfico y se desvió de la carretera con temperaturas bajo cero[64].

Ha llegado el día del dron y sitios web como DIY Drones han establecido

inmensas comunidades dedicadas a construir VANT personales. Para los consumidores, empresas y el gobierno, los drones se han vuelto asequibles, con precios en torno a varios cientos de dólares para los modelos básicos, y vienen cargados de sensores de alta potencia como cámaras HD cuyos canales de vídeo el usuario puede consultar en su teléfono móvil. Pese a que los drones cada vez son más populares y se utilizan para bien, plantean una serie de problemas que van más allá de los asuntos relativos a la privacidad mencionados con anterioridad. En breve nuestros cielos estarán infestados de estos dispositivos y recordaremos con añoranza los tiempos en los que podíamos alzar la vista y ver el azul del cielo, sin legiones de cuadricópteros con pancartas de Pepsi, Viagra y Coppertone, en lo que se está convirtiendo el campo creciente de la «publicidad con drones». El problema se agravará cuando el mundo de la analítica de datos masivos converja con la robótica. Entonces, en lugar de mostrarnos *banners* publicitarios online basados en nuestro historial de búsquedas, *cookies* y «Me gusta» de Facebook, drones con anuncios personalizados se plantarán frente a la ventana de nuestras viviendas o nos perseguirán por las calles portando pancartas publicitarias de verdad. Además, más robots voladores comportarán más accidentes. Si a los pilotos militares entrenados se les han podido caer cuatrocientos VANT del cielo, ¿qué sucederá cuando los adolescentes borrachos de una fiesta universitaria decidan jugar con sus avioncitos?

Y, sin lugar a dudas, si Martha Stewart es capaz de utilizar un dron para vigilar su propiedad y fotografiarla, Crimen, S. A. también puede hacerlo. Los VANT equipados con cámaras no sólo se utilizarán para fines evidentes, como el espionaje industrial y hacer inspecciones antes de cometer hurtos, sino que también ayudarán a los cónyuges celosos a acosar a sus exparejas, incluso en casos de violencia doméstica. Los *hackers* también han averiguado cómo utilizar drones para fines de interceptación de comunicaciones, tanto para pinchar tus llamadas telefónicas como para rastrear todos tus movimientos en Internet, mediante dispositivos como el WASP (siglas en inglés de Wireless Aerial Surveillance Platform o «plataforma de vigilancia aérea inalámbrica»).

Presentado en Las Vegas en 2011, el WASP es un pequeño avión por control remoto con una envergadura de 1,80 metros. Incorpora once antenas y está equipado con diversos sensores y herramientas de comunicaciones, incluida una cámara de alta definición. El WASP está diseñado para sobrevolar el vecindario e interceptar las señales Wi-Fi de quienes nos rodean, incluso de las redes encriptadas. Este dron incorpora un pequeño ordenador Linux a bordo que ejecuta una serie de herramientas de piratería, incluido un diccionario de 340 millones de palabras personalizado, que puede utilizar para generar contraseñas y acceder por la fuerza bruta a tu red en tiempo real. Además, el WASP porta una torre de telefonía móvil fraudulenta que puede utilizar para «hacerse pasar» por proveedores de telefonía móvil GSM[*]. Esta torre de telefonía falsa engaña a tu móvil, que se conecta al WASP y permite a los piratas informáticos grabar todas las llamadas telefónicas y los mensajes de texto que

pasan por el dispositivo[65]. No hace demasiado tiempo, los artilugios para interceptar este tipo de señales con fines de espionaje costaban decenas de millones de dólares y sólo tenían acceso a ellos los Ejércitos más avanzados del mundo. El WASP se construyó por sólo 6000 dólares.

Y ahora que el precio de los drones básicos equipados con cámaras HD ha descendido de manera tan drástica, empiezan a aparecer en los lugares más imprevistos, como en manifestaciones y disturbios. En Varsovia, Polonia, los manifestantes del movimiento Occupy lanzaron un cuadricóptero para documentar la agresiva actuación policial contra los manifestantes, que empleó gases lacrimógenos para intentar controlar a la multitud. El apodado «Ocucóptero» sobrevoló el lugar a unos cien pies del suelo y proporcionó a los manifestantes imágenes de una nitidez asombrosa de los agentes de policía que avanzaban en formación de columna para intentar rodear la manifestación, una herramienta potente y previamente inconcebible de contravigilancia ahora en manos de la gente corriente[66]. Huelga decir que la policía no será la única que deberá bregar con cómo responder de manera adecuada a que la sobrevuelen drones.

Crimen, S. A. también utiliza robots voladores como herramienta predilecta para pasar de contrabando armas, teléfonos móviles y narcóticos a instalaciones correccionales de todo el mundo. En el Centro de Detención Provisional São José dos Campos de São Paulo, Brasil, los agentes del correccional observaron a un dron cuadricóptero sobrevolar los muros de la prisión y dejar caer un pequeño paquete en el patio del recreo de las instalaciones, dentro del cual encontraron 250 gramos de cocaína[67]. A las afueras de Moscú, fue un helicóptero por control remoto el que dejó caer 700 gramos de cocaína en la prisión de Tula. En Grecia se entregó una caja de teléfonos móviles, y se ha informado de intrusiones similares en cárceles de Canadá, Australia y Estados Unidos. Crimen, S. A. está montando lentamente su fuerza aérea robótica.

Un aspecto importante es que el auge de los VANT usados con fines delictivos es completamente incompatible con los paradigmas de seguridad vigentes. Las prisiones emplean altas y afiladas verjas, a menudo eléctricas, para aislar a los delincuentes por motivos de seguridad pública, un sistema que ha funcionado relativamente bien durante siglos. Pero nuestros mecanismos de seguridad y defensa estaban destinados a protegernos de los delincuentes humanos, no de los robóticos. Tal vez haya llegado el momento de replanteárnoslo. Los drones no sólo son capaces de eludir la verjas de las cárceles, sino todas, incluidas las que protegen el patio trasero, un edificio de oficinas e incluso las fronteras nacionales, tal como están demostrando los sindicatos del narcotráfico de Latinoamérica. En México, por ejemplo, Crimen, S. A. ha contratado obreros de cadenas de montaje de las fábricas de aeronáutica locales, quienes se pluriemplean diseñando VANT para los cárteles. En el distrito de Santa Fe, en México, D. F., cerca de la fábrica Bombardier, se descubrió una fábrica secreta de drones para narcotráfico, de acuerdo con el Secretariado para la Seguridad Pública

mexicano. Tomando como referencia diseños estadounidenses, europeos e israelíes, estas aeronaves autónomas y ultraligeras son mucho más grandes que el cuadricóptero medio, pesan varios centenares de kilos y presentan alas plegables que permiten transportarlas fácilmente y ocultarlas en camiones a ambos lados de la frontera. Vuelan a baja altura y resultan indetectables para el radar. Cada dron puede transportar cien kilos de cocaína por trayecto, cocaína que cuesta 1700 dólares el kilo en Colombia, 8000 dólares en México y 30 000 en Estados Unidos, lo cual genera unos ingresos netos para los traficantes de más de dos millones de dólares por vuelo. Desde 2012, la DEA ha documentado al menos 150 cruces de frontera de «narcodrones» que transportaban múltiples toneladas de cocaína[68]. Con beneficios de este calibre, los cárteles desde Cali hasta Sinaloa están reinvirtiendo sus beneficios en investigación y desarrollo avanzados y gastan millones para asegurarse de dotar de una función mucho más prominente a su mano de obra de robots delincuentes en el futuro.

Aparte de drogas, hay otros artículos mucho más alarmantes que los delincuentes avezados en tecnología pueden acoplar a los drones, incluidas armas de fuego[69]. En YouTube abundan ya los vídeos de aficionados que muestran robots voladores construidos por ellos mismos y controlados a distancia, los cuales realizan tareas elaboradas como perseguir y disparar a personas con pistolas de agua y bolas de pintura, un pasatiempo ideal para su adaptación a fines criminales o terroristas. Otros vídeos muestran a aficionados haciendo volar drones con armas paralizantes a bordo que con descargas eléctricas de 80 000 voltios abaten a su presa[70]. Ahora bien, como es de suponer, esta tendencia no acaba aquí, sino que también se han utilizado armas de verdad. El primer vídeo de un arma de fuego real, en el que se veía una pistola del calibre .45 montada en un helicóptero por control remoto y disparando, se remonta a 2008[71]. Desde entonces han aparecido multitud de vídeos en los que se ven VANT con armas controlados mediante *smartphones*, incluida una versión en alta definición de un octocóptero portando un revólver Colt del calibre 45 que se dispara repetidamente mediante un dedo robótico controlado a distancia que aprieta el gatillo[72]. Con las llamadas tecnologías automáticas «sígueme», incluso pueden rastrear de manera autónoma a una persona concreta mientras corre por la calle. Utilizar un teléfono inteligente para disparar un arma real montada en un robot volador que cuesta unos cuantos cientos de dólares implica que los juegos de tiradores en primera persona acaban de llegar al espacio tridimensional y se han convertido en una realidad[73]. ¿Cuánto tardará el primer delincuente o perturbado mental en utilizar un dispositivo de esta índole para asesinar a alguien?

Por peligroso y temible que pueda resultar tal panorama, existen aún otras cargas, mucho más dañinas, que pueden colocarse a bordo de los drones, incluso explosivos y armas de destrucción masiva, como armas biológicas, químicas o radiológicas. Por menos de 20 dólares pueden encontrarse en Internet sistemas de lanzamiento de bombas para aviones por control remoto, similares a las puertas de los bombarderos

militares que se abren cuando se accionan por control remoto o cuando alcanzan un punto de navegación concreto con el GPS. ¿Podrían los drones convertirse en los próximos bombarderos suicidas? Al Qaeda, Lashkar-e-Toiba y otras muchas organizaciones terroristas ya han puesto en marcha programas de fabricación de drones. Varios vídeos en YouTube muestran a agricultores que, cansados de trabajar bajo un sol extenuante, han convertido sus helicópteros por control remoto en aviones fumigadores[74]. Si un terrorista decidiera aplicar la misma idea para propagar una sustancia letal sobre una multitud en lugar de pesticidas sobre campos de arroz, el potencial de provocar daños sería enorme.

Los drones, tal como nos ha demostrado el Ejército, también pueden utilizarse de modos dirigidos con precisión contra personas concretas, ya sea por venganza personal, ya como acto criminal o terrorista. Ya hemos empezado a ver cómo personas de alto nivel son atacadas de modos extraños y peligrosos. A finales de 2013, la canciller alemana Angela Merkel fue atacada por un dron durante un mitin de campaña en Dresde, ataque en el que un VANT cuadricóptero se dirigía hacia ella mientras estaba en el escenario, si bien se estrelló a sus pies. El ataque lo llevó a cabo el Partido Pirata alemán, que, según confirmó, quería asegurarse de que la canciller supiera «lo que significa estar subyugado a la observación con drones»[75]. Los encargados de la protección de Merkel sin duda captaron el mensaje. Aunque nadie resultó herido a causa de aquella estratagema, la noticia podría haber tenido un final mucho menos feliz en caso de haber ido armado el dispositivo o de portar explosivos.

Los drones también pueden provocar daños cuando se lanzan contra otros medios de transporte, de manera que desconciertan a los conductores de automóviles y provocan accidentes. Ya existen en todo el mundo numerosas denuncias de aficionados que han colocado de manera intencionada drones voladores en la ruta de vuelo de un avión y han obligado a los pilotos a acciones evasivas drásticas para evitar colisionar con ellos, incluidos aviones de American Airlines, US Airways, Alitalia y Virgin Blue[76]. En caso de que alguno de estos robots voladores hubiera sido succionado por los motores del avión comercial, podría haber provocado un accidente similar al que derribó al avión de pasajeros de US Airways sobre el río Hudson de Nueva York. A medida que transcurra el tiempo y robots voladores, nadadores, rodantes y caminantes se internen en nuestras vidas, tendremos que determinar nuevas maneras de convivir de manera segura y pacífica con ellos, si bien el futuro de la robótica podría plantear riesgos aún más importantes que habrá que afrontar.

El futuro de las máquinas robóticas y autónomas

Los robots se volverán más rápidos, más inteligentes y más pequeños. Ya se están realizando grandes procesos en la microrrobótica[77]. Los dispositivos, algunos de ellos tan pequeños como la yema de un dedo, se controlan de manera remota y pueden estar equipados con un micrófono y una cámara HD, lo cual lleva las cuestiones acerca de la privacidad y la vigilancia a todo un nuevo nivel[78]. Ya existen noticias de drones libélula utilizados para espiar a los manifestantes pacifistas en Washington, D. C., en 2007, y las Fuerzas Aéreas desvelaron abejorros robóticos que no serían detectados en entornos hostiles mientras entraban volando en edificios para «fotografiar, grabar e incluso atacar a terroristas»[79].

Otro gran avance inminente en la robótica será la posibilidad de formar «enjambres», es decir, reunir múltiples robots en sistemas para que actúen al unísono mediante un comportamiento colectivo que imite la naturaleza, del mismo modo que las hormigas colaboran y las aves vuelan en bandadas. Aplicando el poder de la computación distribuida avanzada para autoorganizarse y solventar problemas, enjambres de robots podrían coordinar sus esfuerzos para conseguir cosas increíbles tanto en operaciones de ayuda tras una catástrofe como de búsqueda y rescate, vertidos de petróleo o fabricación. Se están registrando grandes avances en la inteligencia de los enjambres y, a mediados de 2014, un equipo de investigación de la Harvard University creó el enjambre de robots más extenso de la historia, integrado por 1024 robots minúsculos del tamaño de un penique capaces de encontrarse entre sí y colaborar para componer varias formas y diseños, incluidas letras y estrellas, como si se tratara de una multitud de máquinas que empiezan a bailar de improviso al unísono[80]. Sin embargo, puede que el enjambre de robots colaboradores y autoorganizados que se forme en el horizonte sea una fuerza del mal. Que un dron te persiga con un revólver por una calle ya es bastante malo, pero que lo haga un enjambre de treinta drones no sólo resultaría aterrador, sino que las posibilidades de sobrevivir serían mínimas. Más aún, una vez se extienda el uso de los enjambres de robots, cualquier pirateo o virus al que se vean sometidos podría tener unas consecuencias nefastas, pues afectaría a todos los *bots* de la red, como en las escenas descritas en la serie televisiva *Star Trek* donde la tripulación de la *Enterprise* utiliza un virus informático para destruir efectivamente el colectivo de organismos cibernéticos Borg, salvo por el hecho de que nosotros podríamos ser el Borg destruido. Cuando el Ejército extienda el uso de VANT armados que operen en formación a modo de enjambre en sus ataques contra el enemigo, en el caso de que los infecte un virus (tal como ha sucedido con el centro de mandos de los drones estadounidenses), ¿con qué facilidad podrán volverse los robots voladores armados contra sus dueños o contra poblaciones civiles inocentes?

Y a medida que continúe el progreso no sólo veremos enjambres de robots cada vez más pequeños a nuestro alrededor, sino que esos robots serán cada vez más autónomos, máquinas inteligentes capaces de realizar tareas y adoptar decisiones en el mundo real por sí mismas, sin un control humano explícito. Un robot autónomo,

como el aspirador Roomba, toma decisiones en función de su programación, pero en su propio tiempo real, aplicando algoritmos de «chocar y continuar» para desplazarse y evitar obstáculos, algoritmos que le permiten analizar y adaptarse a entornos con los que no está familiarizado.

Con todo, las preguntas más espinosas guardan relación con la robótica militar: ¿dónde se pone el límite? Un ejército de médicos robóticos terrestres capaces de rescatar de manera autónoma a un soldado herido del campo de batalla y proporcionarle unos primeros auxilios que le salven la vida suena sensacional. Pero la idea de que un VANT pueda localizar su objetivo y de manera autónoma tomar la decisión de disparar a matar haría que muchos se lo pensaran dos veces. Y, sin embargo, ahí es exactamente adonde nos dirigimos. A medida que la robótica, la inteligencia artificial y las velocidades de procesamiento informático mejoren de manera exponencial, en algún punto los seres humanos sencillamente no seremos lo bastante rápidos como para estar al día, sobre todo en el ámbito de la guerra. Una vez el enemigo desencadene una guerra completamente anónima, no quedará más remedio que hacer lo mismo o afrontar la destrucción.

Pese a que puedan parecer propias de películas distópicas y apocalípticas como *The Terminator*, las máquinas voladoras autónomas ya existen. El BAE Systems Taranis es un avión totalmente autónomo que puede «adentrarse volando en territorio enemigo para recopilar información privilegiada, arrojar bombas y "defenderse de otros aviones tanto tripulados como no tripulados"»[81]. En la zona desmilitarizada al otro lado de la península de Corea, Corea del Sur ha desplegado robots francotiradores de control fronterizo Samsung SGR-1 capaces de detectar a intrusos mediante sensores de calor y movimiento y de disparar automáticamente contra objetivos desde hasta un kilómetro de distancia con sus metralletas de 5,5 mm incrustadas y sus lanzagranadas de 4 mm. Pese a que estos robots de fronteras actualmente requieren autorización humana para atacar por razones políticas, técnicamente pueden ser completamente autónomos con sólo accionar un interruptor[82]. Los robots asesinos autónomos y letales adoptarán múltiples formas: máquinas andadoras, nadadoras, voladoras y conductoras capaces de perseguir a su presa o, sencillamente, de permanecer al acecho. Mas, pese a nuestra creciente capacidad técnica para delegar decisiones asesinas en máquinas, hacerlo conlleva multitud de implicaciones legales, éticas, morales, técnicas y de seguridad.

Los accidentes industriales con robots son terribles, pero, como demuestra lo sucedido a causa de aquel espantoso error informático de la Fuerza de Defensa sudafricana, los accidentes con robots dotados de armas automáticas pueden ser catastróficos. A medida que los robots proliferen y que la ley de Moore choque con la ley de Murphy, padeceremos las consecuencias. Una mala programación, datos imprecisos y errores de *software* sin duda desembocarán en tragedia cuando los robots puedan decidir por sí mismos matar. Más aún, los robots conectados a la Internet de las Cosas podrán piratearse, como también podrán piratearse sus

funciones y protocolos de seguridad, lo cual añadirá otro peligro notable a tener en cuenta. También es preocupante que gobiernos represivos puedan utilizar robots asesinos para reprimir a los disidentes o que los cárteles del narcotráfico los empleen para asesinar a policías y miembros de bandas rivales. Podría parecer una hipérbole sugerir que Crimen, S. A. contará algún día con robots asesinos autónomos, pero desde luego que lo hará, de la misma manera que ya ha adoptado muchas otras tecnologías previamente militares, incluidas las gafas de visión nocturna, Internet y los drones. A los expertos en derechos humanos y tecnología les preocupa que se deleguen decisiones asesinas en máquinas. De hecho, el tema ha sido planteado por la ONU, el Observatorio de Derechos Humanos (HRW) y nuevas organizaciones como el Comité Internacional para el Control de Armas Robóticas y la Campaña para Detener los Robots Asesinos. El autor de ciencia ficción Daniel Suárez y el roboticista Noel Sharkey han impartido charlas apasionadas en las conferencias TED donde exigen que se prohíba a nivel mundial que los robots puedan asesinar o herir a un ser humano de manera autónoma, una idea realmente sensata, propuesta ya por Asimov hace décadas.

Que los robots formarán parte de todos los ámbitos de nuestras vidas, ya sea para cuidar de ancianos, cocinar o practicar intervenciones quirúrgicas, es ya un hecho. Pueden ser un agente impresionante del bien, pero, tal como hemos visto a lo largo de este capítulo, también pueden caer en manos de mafiosos, mirones, cárteles del narcotráfico y terroristas, una tendencia que seguramente se acelerará a medida que su funcionalidad mejore y su precio descienda, sobre todo a causa de las impresionantes tecnologías nuevas y complementarias, como la impresión 3D.

Imprimir delitos: cuando Gutenberg y Gotti[*] aúnan fuerzas

> Es difícil imponer restricciones en un mundo donde todo el mundo puede hacerlo todo.
>
> HOD LIPSON

La impresión 3D o, como se la denomina a veces, la «fabricación aditiva», promete hacer realidad el replicador de *Star Trek*. Con sólo pulsar un botón, una máquina mágica puede hacer que aparezcan ante nuestros ojos objetos físicos utilizando un amplio abanico de materiales, incluidos el plástico, el metal, la madera, el hormigón, la cerámica y hasta el chocolate. Del mismo modo que se puede imprimir una fotografía con una impresora de chorro de tinta 2D, es posible descargarse o crear un diseño en el ordenador portátil y enviarlo a una impresora 3D, la cual, utilizando

diversas técnicas, es capaz de construir objetos tridimensionales, capa por capa, con una precisión asombrosa. Estas técnicas de fabricación digital están facilitando y abaratando la construcción no sólo de robots, sino de todo un espectro de productos que abarca desde piezas para aeronáutica hasta lentes y cámaras réflex de objetivo único que funcionan a la perfección.

Goldman Sachs ha señalado que, en comparación con la fabricación tradicional, la impresión 3D permitirá una mayor personalización y reducirá los costes de diseño complejos, y hay quien predice un crecimiento del 500 por ciento del mercado de las impresoras 3D de aquí a 2018, con un capital en circulación de 16 000 millones de dólares[83]. En la actualidad, inventores como Scott Summit, fundador de Bespoke Innovations, utilizan impresoras 3D para crear prótesis personalizadas de próxima generación, que no sólo se amoldan a la perfección, sino que, además, presentan diseños de gran belleza. La fabricación digital puede emplearse para imprimir viviendas enteras, con hormigón, cableado eléctrico, tuberías y todo lo necesario[84]. La NASA incluso ha adquirido una impresora 3D para la Estación Espacial Internacional a la empresa novel de Silicon Valley Made in Space, con el fin de asegurarse de no tener que preocuparse nunca más de que la pérdida de una pieza a bordo ponga en peligro las vidas de los astronautas, como ocurrió en el caso del *Apollo 13*. Las impresoras de biofabricación nos han adentrado en un nuevo nivel, donde las máquinas son capaces de imprimir órganos y tejidos humanos, como capilares, riñones, oídos y corazones, lo cual podría poner fin a las listas de trasplantes y salvar vidas[85].

Los precios de las impresoras 3D domésticas, máquinas que en el pasado solían costar decenas de miles de dólares, descienden en picado, y ya es posible adquirir modelos como la popular Cube 3 de 3D Systems en Staples por 999 dólares. Amazon ha creado su propia tienda de impresión 3D y sitios web como Thingiverse se han convertido en parada obligatoria para que los usuarios compartan y personalicen libremente sus archivos de diseño digital para poder crear cualquier cosa, desde joyería hasta fundas para el iPhone, y MakerBot ofrece kits para montar incluso tu propia impresora 3D. El *software* y las aplicaciones gratuitas de Autodesk 123D pueden convertir una maqueta digital 3D en un objeto del mundo real y su sistema operativo de código abierto, Spark, podría ser a las impresoras 3D lo que Android es a los teléfonos inteligentes. Estos avances podrían alejar la fabricación de la producción en serie y encauzarla hacia la personalización masiva, que permitiría a los consumidores imprimir exactamente el zapato, la mesa o el juguete que les gusta. Chris Anderson, el antiguo editor jefe de *Wired* editor, ha documentado de manera excelente este llamado «movimiento del bricolaje digital» en su libro *Makers*, donde menciona el diseño de código abierto y la fabricación digital como los cimientos de la nueva revolución industrial.

Otro aspecto destacable de las impresoras 3D es que estos dispositivos avanzan hacia una autorreplicación total. En la actualidad, la mayoría de las impresoras 3D

son capaces de imprimir más del 50 por ciento de las piezas necesarias para fabricar otra impresora 3D, y ese porcentaje se incrementa a toda máquina[86]. Las impresoras permiten transmitir objetos físicos a través de Internet e imprimirlos bajo demanda. Las impresoras 3D, como la robótica y la Internet de las Cosas, nos están internando en una era en la que lo analógico y lo digital se están fusionando y se vuelven indiferenciables uno de otro. Bits y *bytes* devienen átomos y los escáneres 3D, como el Kinect de Microsoft, pueden transformar objetos físicos en unos y ceros. El resultado podrían ser inmensas interrupciones en la fabricación, venta al por menor e incluso geopolítica. La fabricación y el montaje locales podrían tener unas repercusiones positivas inmensas para el medio ambiente. Si puedes imprimir lo que necesitas en casa, ¿por qué bajar a la tienda? Y si las empresas estadounidenses pueden imprimir más de lo que necesitan en territorio nacional, ¿qué sentido tiene enviar montones de plástico barato a través de los océanos desde China? Al margen de cómo evolucionen estas transformaciones, hay un colectivo que ha recibido con los brazos abiertos este movimiento del bricolaje digital: Crimen, S. A.

Tal como la robótica ha entrañado nuevos ciberriesgos para el mundo tridimensional en el que habitamos, la fabricación digital también comportará los suyos. El primer aspecto en el que se centrarán los delincuentes en el mundo de la impresión 3D es el robo de propiedad intelectual. En el pasado, sólo era posible piratear y duplicar a la perfección la propiedad intelectual digital, ya fuera música, vídeo, juegos o programas de *software*. Pero eso está a punto de cambiar. Pese a que los ladrones llevan haciendo bolsos Gucci falsos y copias de relojes Cartier desde hace tiempo, resultaban relativamente fáciles de detectar debido a su diseño chapucero y a su fabricación barata. En cambio, en el futuro estos objetos estarán sujetos a un escaneado e impresión en 3D de ultra alta resolución, lo cual redundará en que las copias tendrán la misma calidad que el original. El grupo Gartner ha vaticinado que la impresión 3D comportará más de cien mil millones de dólares en pérdidas de propiedad intelectual anuales a nivel mundial hacia 2018[87].

La fabricación digital también será una bendición para los ladrones y acosadores que ahora podrán tomar una fotografía de alta resolución de las llaves de una vivienda u oficina que hayas dejado sobre tu escritorio y utilizar un servicio como KeyMe para imprimir un duplicado del juego de llaves mediante el mercado de la impresión 3D Shapeways[88]. También existen aplicaciones, como Keys Duplicated, que permitirán hacer lo propio y proporcionarán las llaves de tu castillo a más personas de las que te gustaría[89]. Si te inquieta, debes saber que no eres el único. En 2012, la policía descubrió archivos de diseño infográfico en Internet que permiten a los delincuentes fabricar digitalmente llaves para esposas policiales, incluidos modelos ultraseguros cuyos fabricantes no venden llaves al público[90]. En el futuro, tu camello de drogas también podría ser una impresora. Los científicos ya han desarrollado una «quimimpresora» capaz de imprimir bajo demanda medicamentos como ibuprofeno. Si bien los beneficios humanitarios potenciales de este artilugio

son enormes, Crimen, S. A. no tardará en adaptar estas máquinas para fabricar *meth*, *crack* y oxicontina, con lo cual simplificará de manera sensacional los problemas relacionados con la cadena de suministros y distribución[91].

Quizá uno de los aspectos más polémicos que envuelven a las impresoras 3D sea su capacidad de producir armas de fuego, muestra de lo cual nos dio Cody Wilson, un antiguo estudiante de Derecho de veintiséis años anarquista y libertario al estilo del Temible Pirata Roberts. Wilson creó el Wiki Weapon Project, inventó el Darkwallet y su criptomoneda imposible de rastrear, y fundó Defense Distributed, un servicio sin ánimo de lucro de diseño, edición y depósito de copias cianográficas de armas en Internet que pueden descargarse e imprimirse con una impresora 3D[92]. Entre sus creaciones impresas en 3D figuraba un receptor bajo para un rifle semiautomático AR-15 con el cual disparó seiscientas ráfagas de munición. El receptor bajo es la pieza clave del arma y la única regulada por ley; el resto de las piezas pueden obtenerse en muchos estados de Estados Unidos sin comprobación del historial delictivo e incluso sin identificación[93]. En mayo de 2013, Wilson también diseñó el Liberator, la primera arma totalmente impresa en 3D, concebida para disparar balas de revólver del calibre 380, y 100 000 personas en todo el planeta se han descargado ya los dibujos[94]. Cuando la prensa le preguntó qué opinaba acerca de su logro, Wilson replicó que ahora «allá donde haya un ordenador y una conexión a Internet, existirá la promesa de un arma».

Los esfuerzos de Wilson han dejado atrás al Congreso, que no aprobó el proyecto de ley que prohibía las armas impresas en 3D[95]. Estas armas de plástico pueden resultar casi imposibles de detectar por los detectores de metal estándares, tal como demostró un equipo de investigadores israelíes al entrar de contrabando una pistola 3D en el edificio de alta seguridad del Knéset, la Asamblea de Israel, y no en una, sino en dos ocasiones[96]. Entre tanto, docenas de armeros digitales adicionales han mejorado el Liberator original e incluso han publicado sus propios archivos de armas digitales en Internet. Han aparecido otros depósitos en línea de diseños de armas 3D, incluidos algunos que incluyen planos para granadas y sistemas de mortero[97]. El Centro Analítico de Dispositivos Explosivos Terroristas del FBI ha manifestado su preocupación ante esta tendencia y recientemente adquirió su propia impresora 3D para investigar cómo pueden utilizar los terroristas estos aparatos para construir dispositivos explosivos improvisados[98]. El enigma en cuanto a armamento se refiere que plantean las impresoras 3D, además, no es estático, ya que, a medida que estos dispositivos aumenten de tamaño y capacidad, serán capaces de fabricar incluso armas de mayores dimensiones, incluidos lanzamisiles de hombro y grandes robots de estilo militar.

Con la fabricación digital, las inspecciones fronterizas nacionales se volverán un sinsentido. ¿Por qué arriesgarse a pasar de contrabando armas o drogas a un país si puedes imprimir revólveres, pastillas o bombas después de cruzar la frontera? Los

desafíos que plantea la impresión 3D a la seguridad internacional no se limitan a los delitos y el terrorismo, sino que también afectarán a instrumentos de toda la vida de la ley internacional, como las prohibiciones de armas. ¿Que a Irán le hacen falta piezas para sus centrifugadoras de uranio? Ningún problema, se imprimen. Los embargos e incluso los bloqueos navales, hasta la fecha las herramientas tradicionales para velar por la seguridad internacional frente a regímenes corruptos, fracasarán de manera épica a medida que las impresoras de mayor tamaño y más sofisticadas se generalicen. Los viejos paradigmas de guardas, vallas y verjas altas y fronteras nacionales quedarán desfasados, pues la tecnología evoluciona mucho más rápidamente que nuestros mecanismos de seguridad… y la nueva normalidad se verá aún más exacerbada por toda una serie de tecnologías nuevas propias de la ciencia ficción que poblarán Internet en un futuro muy cercano.

Capítulo 16

Amenazas de seguridad de nueva generación, o por qué lo virtual no era más que el principio

> Hemos organizado las cosas de modo que casi nadie entienda la ciencia y la tecnología, lo cual es la receta perfecta para el desastre. Es posible que nos las apañemos durante un tiempo, pero tarde o temprano esta mezcla explosiva de ignorancia y poder nos va a estallar en la cara.
>
> CARL SAGAN

«Última hora: dos explosiones en la Casa Blanca. Barack Obama, herido», informó Associated Press en una actualización de su cuenta oficial de Twitter a las 13.07 hora del 23 de abril de 2013. En un instante, sus dos millones de seguidores habían efectuado miles de retuits de la noticia y el mundo se dejó llevar por el pánico. En Wall Street, la reacción fue tan rápida como impactante: el índice Promedio Industrial Dow Jones y el S&P 500 se desplomaron. En sólo tres minutos, el tuit de AP había hecho desaparecer ciento treinta y seis mil millones de dólares en valores accionariales.

A partir de ahí, los tuits se propagaron con rapidez y viveza. A las 13.13 horas, AP confirmó que el explosivo tuit informativo era falso. A las 13.16 horas, el secretario de prensa de la Casa Blanca, Jay Carney, se vio obligado a declarar en directo por la televisión: «Puedo afirmar que el presidente está bien; acabo de estar con él». Finalmente, a las 13.17 horas, el Ejército Electrónico Sirio (SEA en sus siglas inglesas) admitió haber pirateado a Associated Press. En cuestión de nueve minutos, el SEA había conseguido convulsionar algunas de las instituciones más poderosas del mundo, desde Wall Street hasta la Casa Blanca, con un tuit incontrolable. ¿Qué demonios acababa de ocurrir?

Cuando se dio la noticia de que había habido una explosión en el número 1600 de la avenida Pennsylvania, los mercados sospecharon que se trataba de un ataque terrorista y de inmediato anticiparon el profundo impacto negativo que éste tendría; al fin y el cabo, se estima que el 11-S supuso para Estados Unidos unas pérdidas económicas de 3,3 billones de dólares. Los agentes de bolsa empezaron de inmediato a deshacerse de sus acciones y los parqués entraron en caída libre. Pero estos agentes no eran Gordon Gekko, esos tipos del pasado que se creían los amos del universo, con el pelo engominado y trajes de diez mil dólares. De hecho, ni siquiera eran humanos. En los fondos de cobertura, los bancos de inversiones y los fondos de pensiones de las zonas triestatales y de todo el mundo, las redes y los superordenadores realizaron esas operaciones en masa, esclavizados por su

programación algorítmica.

En 1999, Gekko y la mayoría de los que como él se dedicaban al mercado de valores perdieron su prominencia y fueron sustituidos por plataformas de negociación de alta frecuencia (HFT en sus siglas inglesas) ultrarrápidas y electrónicas. Estos algoritmos (*algos*) son una forma de inteligencia artificial, autorizada a tomar decisiones de mercado y gastar dinero en beneficio de sus clientes. En 2015, representan el 70 por ciento del volumen de operaciones del Dow Jones. Estos programas de *software* (programados por seres humanos) llevan a cabo detallados cálculos y razonamientos automatizados con el fin de responder a las fluctuaciones del mercado y analizan las noticias codificadas en lenguaje informático para obtener los máximos beneficios para sus dueños. En términos simplistas, los beneficios trimestrales de una empresa significan comprar, y un ataque terrorista significa vender. Los superordenadores que hay detrás de las plataformas de negociación son lectores voraces que trabajan las veinticuatro horas, los siete días a la semana para descubrir pedazos de información que pueden provocar movimientos en los mercados. Un único servicio de noticias, Thomson Reuters, alimenta estos algos HFT analizando cincuenta mil fuentes periodísticas distintas y cuatro millones de páginas de redes sociales a una velocidad que no podría igualar ningún ser humano. Las amplias redes de las máquinas HFT pueden realizar de forma colectiva billones de cálculos por segundo, y las compraventas pueden efectuarse en menos de una millonésima de segundo, miles de veces más rápido que un parpadeo.

Cuando los *bots* algorítmicos de cambio basados en inteligencia artificial se encontraron con un tuit en el que se citaban en la misma frase las palabras «explosiones», «Obama» y «Casa Blanca», procedente de una fuente en la que por programación confían, Associated Press, tardaron tan sólo milésimas de segundos en reaccionar. Al hacerlo, otros algoritmos se percataron de la actividad y no tardó en generarse un efecto de bola de nieve. Los algoritmos empezaron a vender en masa, haciendo desaparecer valores que ascendían a 136 000 millones de dólares en un tiempo sorprendente: tres minutos. Cualquier ser humano que hubiera leído con atención el tuit se habría dado cuenta de que su redacción era mala, el formato no era propio de AP y las palabras «última hora» no estaban escritas con mayúsculas, como marca el libro de estilo de la agencia de noticias. Todas estas sutilezas pasaron inadvertidas a un agente bolsa robótico. Para entonces, sin embargo, el mal ya estaba hecho. En cuanto pasó la tormenta, muchas empresas habían perdido millones de dólares. El Ejército Electrónico Sirio, un grupo de piratas informáticos internacional con vínculos con el régimen de Bashar al-Assad, asumió la autoría del ataque y se burló del presidente con el *hashtag* #byebyeObama en su propia cuenta de Twitter, @official_SEA6. También compartieron alegremente con el mundo la contraseña de la cuenta de AP en Twitter: APM@*rketing*. El FBI y los funcionarios de seguridad ya se habían cruzado con anterioridad con el SEA, cuando éste pirateó el *New York Times*, la BBC y CBS News, pero su último ataque bastó para incluirlo en el listado

de organizaciones terroristas y en la lista de los más buscados del FBI.

La debacle generada por el tuit de la AP sobre la explosión en la Casa Blanca no fue la primera ocasión en que los algoritmos causaron estragos en Wall Street, y seguro que no será la última. Más importante aún, una investigación de la Securities and Exchange Commission de esta clase de incidentes, incluido el tristemente célebre *Flash* Crash de mayo de 2012, concluyó que el mercado, dominado por algoritmos de compraventa ultrarrápidos, «se había vuelto tan fragmentado y frágil que un único gran volumen de intercambios podía provocar una caída vertiginosa y repentina de las acciones»[1]. En un mundo que ahora se mide en millonésimas de segundo y cuya velocidad aumenta de manera exponencial, no existe literalmente posibilidad de intervención humana una vez que los *algos* comienzan a fallar. La capacidad del Ejército Electrónico Sirio de convulsionar los mercados financieros internacionales en un solo instante pone al descubierto los riesgos del ciberterrorismo en un mundo hondamente interconectado, automatizado por ordenadores y que opera casi a la velocidad de la luz. Pero esta historia refleja mucho más que una simple anécdota trágica acerca del peligroso estado de nuestra seguridad económica común: es un presagio de lo que está por venir. Nos demos cuenta o no, cada vez entregamos una parte mayor de nuestras vidas a algoritmos informáticos e inteligencias artificiales para que tomen decisiones por nosotros. Para aquellos que recuerden la desagradable relación de John Connor con Skynet en la película *Terminator*, se trata de una decisión plagada de riesgos.

Casi inteligentes

> La cuestión de si un ordenador se dedica a jugar al ajedrez, hacer una larga división o traducir del chino es equiparable a la cuestión de si los robots pueden asesinar o los aviones volar… Se trata de cuestiones relacionadas con las decisiones, no con los hechos; la decisión de adoptar una extensión metafórica del uso habitual.
>
> NOAM CHOMSKY

Cuando el científico informático John McCarthy acuñó el término «inteligencia artificial» en 1956, la definió sucintamente como «la ciencia y la ingeniería para fabricar máquina sinteligentes». Hoy en día, la inteligencia artificial (IA) se refiere en un sentido más amplio al estudio y la creación de sistemas informáticos capaces de llevar a cabo tareas que se asemejan a la capacidad humana para resolver problemas, mediante el uso de algoritmos informáticos para hacer cosas que por lo general requerirían la inteligencia humana, como el reconocimiento de la voz, la percepción visual o la toma de decisiones. Estos ordenadores y agentes de *software* no tienen conciencia de sí mismos o inteligencia como las personas; más bien son herramientas

que llevan a cabo funciones codificadas en su interior y heredadas de la inteligencia de sus programadores humanos. Éste es el mundo de la IA débil o estrecha, y vivimos rodeados de ella.

La IA débil puede ser un medio muy poderoso para realizar tareas específicas y estrechas. Cuando Amazon, TiVo o Netflix te recomiendan un libro, un programa de televisión o una película, lo hacen basándose en tus compras previas, repasando el historial y los datos demográficos que manejan sus algoritmos de IA. Cuando recibes una llamada telefónica automatizada de la empresa de tu tarjeta de crédito para avisarte de un posible fraude en tu cuenta, es la IA la que dice: «Vaya, normalmente Jane no compra cosméticos en Manhattan y tan sólo media hora después un ordenador portátil en Lagos». El traductor de Google no podría funcionar sin IA, ni tampoco el GPS de tu coche o tus conversaciones con Siri.

Hable con mi agente

> La tecnología, al fin y al cabo, no es más que la manifestación física de la voluntad humana y, en lo que se refiere a los agentes de IA, ese humano puede aumentar digitalmente mil millones de veces. Ya seas un agente de bolsa de alta frecuencia de Wall Street, un creador de *software* malicioso, un investigador médico, un agente de comercialización, un astrónomo, un dictador o un constructor de drones, la IA estrecha es el caballo de tiro de la era de la automatización.
>
> DANIEL SUAREZ

Cuando programas tu DVR para que grabe el último capítulo de *Mad Men* o la alarma del iPhone para que te despierte a la siete de la mañana, de hecho estás programando un *software* para que se comporte como un agente inteligente en tu lugar. La IA es un *software* al que le confieres voluntad de acción para que te represente en otro lugar de la sociedad. Con el tiempo, acabaremos por confiar en esta clase de «botlers» para que nos ayuden con casi todas las tareas de nuestras vidas, desde las más cotidianas hasta las trascendentales.

A medida que se incrementan las capacidades de la IA estrecha, asistimos a un aumento del papel activo de los algoritmos en todos los negocios y profesiones. En medicina, los «diagnósticos asistidos por ordenador» ayudan a los médicos a interpretar radiografías, imágenes por resonancia magnética y ecografías con mayor rapidez, mediante el uso de algoritmos y técnicas de reconocimiento de patrones complejos que alertan sobre resultados anormales en las pruebas. Vinod Khosla, el legendario emprendedor e inversor de Silicon Valley, se ha referido a nuestra época como la era del doctor A. (doctor Algoritmo), que provocará una revolución en la asistencia médica en la que los doctores humanos ya no serán necesarios, pues entre

el 90 y el 99 por ciento de nuestras necesidades de atención sanitarias serán atendidas de forma mucho más rápida y barata gracias a la IA, los datos masivos y *software* y diagnósticos médicos mejorados[2]. Los médicos no son los únicos que se enfrentan a una significativa alteración de su práctica debido a la competencia de los algoritmos: ejércitos enteros de costosos abogados están siendo remplazados por *software* más barato. Hoy en día, el *software* de inteligencia artificial e-discovery puede analizar millones de documentos de la instrucción de un juicio, cribándolos, clasificándolos y ordenándolos según su valor potencial como pruebas a una velocidad que ningún abogado humano podría igualar, y todo por un 15 por ciento del coste[3]. Pero ¿qué sabemos en realidad de estos algoritmos y de los procesos matemáticos que los conforman? Resulta que muy poco.

Algoritmos de caja negra y la falacia de la neutralidad matemática

Uno más uno son dos. Dos más dos son cuatro. Matemáticas básicas, eternas, inmutables; la clase de cosas que aprendimos en el parvulario. Pero existe otra clase de matemáticas: las matemáticas codificadas en los algoritmos, fórmulas escritas por humanos y programadas para seguir sus instrucciones y orientaciones, y llevar a cabo sus análisis para tomar decisiones. Cuando tu GPS te proporciona indicaciones utilizando IA estrecha para procesar la petición, está tomando decisiones por ti sobre la ruta basándose en un conjunto de instrucciones que alguien ha programado. Aunque haya cien formas distintas de ir de tu casa al despacho, tu sistema de navegación ha elegido una. ¿Qué ha pasado con las noventa y nueve restantes? En un mundo manejado cada vez más por algoritmos, no se trata de una cuestión intrascendente o sin importancia.

En la actualidad disponemos de:

- comercio algorítmico en Wall Street (*bots* que se ocupan de comprar y vender);
- justicia delictiva algorítmica (radares de velocidad y en los semáforos con cámaras incorporadas para detectar infracciones);
- control de fronteras algorítmico (la IA puede señalarte a ti y a tu equipaje para que os registren);
- puntuación de crédito algorítmica (tu puntuación FICO determina tu solvencia);
- vigilancia algorítmica (las cámaras de CCTV pueden identificar actividades inusuales mediante análisis visual computarizado, y el sistema de reconocimiento de voz puede analizar tus llamadas telefónicas en caso de problemas con las contraseñas);

- sistema sanitario algorítmico (tanto si se aprueba tu petición de ver a un especialista o tu reclamación al seguro como si no);
- guerras algorítmicas (los drones y otros robots tienen la capacidad técnica de encontrar, fijar como objetivo y matar sin intervención humana), y
- citas algorítmicas (páginas web como eHarmony se comprometen a encontrar tu alma gemela o tu pareja perfecta usando las matemáticas).

Aunque a los inventores de estas fórmulas algorítmicas les encantaría afirmar que éstas son totalmente neutras, nada más alejado de la realidad. Cada algoritmo está impregnado del profundo sesgo humano de la persona o personas que escribieron la fórmula. Pero ¿quién gobierna estos algoritmos y su comportamiento al ocuparse de nosotros? No tenemos ni idea. Se trata de algoritmos de caja negra, rodeados de secreto y a menudo declarados secretos industriales, protegidos por la ley de propiedad intelectual. Un único algoritmo —la puntuación FICOF— juega un papel fundamental en el acceso al crédito de cualquier estadounidense, en su posibilidad o no de conseguir una hipoteca y en la tasa del crédito para comprar un coche[4]. Pero la fórmula no está publicada en ninguna parte; de hecho, es un secreto preservado con celo que proporciona a FICO cientos de millones de dólares de beneficios al año. Pero ¿y si hubiera un error en los datos o los supuestos inherentes al algoritmo? Mala suerte para ti. La falta de transparencia casi absoluta de los algoritmos que manejan el mundo implica que vivimos sumidos en la ignorancia y que no tenemos nada qué decir acerca de decisiones de gran importancia que se toman sobre y por nosotros. El creciente poder concentrado de los algoritmos en nuestra sociedad ha pasado inadvertido para la mayoría, pero sin conocimiento y transparencia de los algoritmos que hacen funcionar el mundo no puede existir responsabilidad o verdadera democracia. Como resultado, la sociedad del siglo XXI que estamos construyendo es cada vez más susceptible de manipulación por parte de aquellos que crean y controlan los algoritmos que rigen nuestras vidas.

Un ejemplo flagrante de este abuso se reflejó en un estudio publicado a mediados de 2014 por investigadores de Facebook y la Universidad de Cornell, que revelaba que las redes sociales pueden manipular las emociones de sus usuarios simplemente alterando lo que ven en el canal de noticias. En un estudio publicado por la Academia Nacional de Ciencias estadounidense, Facebook cambió la actualización del canal de setecientos mil usuarios para mostrarles noticias más tristes o más alegres[5]. ¿El resultado? Los usuarios que veían noticias más negativas se sentían peor y escribían publicaciones más negativas, mientras que a los que veían las noticias más alegres les ocurría lo contrario. Conclusión del estudio: «Los estados emocionales pueden transferirse a otras personas mediante el contagio emocional, que lleva a la gente a experimentar las mismas emociones sin ser consciente». Facebook nunca notificó de forma explícita a los usuarios afectados (entre los que se incluían jóvenes de entre trece y dieciocho años de edad) que habían sido seleccionados sin su consentimiento

para un experimento psicológico[6]. Tampoco tuvo en cuenta aspectos relacionados con la salud mental, como la depresión o la tendencia al suicidio, que pudieran sufrir los usuarios antes de decidir manipularlos cruelmente para que se sintieran aún más tristes. Aunque Facebook actualizó sus condiciones de servicio para otorgarse el permiso de «llevar a cabo investigaciones» *después* de completar el estudio, muchos han argumentado que las actividades del gigante de las redes sociales equivalían a una investigación con sujetos humanos, un marco que habría requerido una aprobación ética previa por parte de una junta de revisión interna que respondiera a las regulaciones federales[7]. Por desgracia, Facebook no es la única empresa que utiliza algorítmicamente a sus usuarios como ratas de laboratorio.

La falta de transparencia algorítmica, combinada con una mentalidad de «En la pantalla confiamos», resulta peligrosa[8]. Cuando se mezclan los datos masivos, la computación en la nube y la inteligencia artificial con la Internet de las Cosas, como sucede ya en la actualidad, el resultado es un número cada vez mayor de objetos físicos que actúan por nosotros en el espacio en tres dimensiones. Que la IA haga que un robot te prepare el café y el desayuno suena genial. Pero si recordamos el homicidio en 1981 de Kenji Urada, un empleado de Kawasaki de treinta y siete años al que un robot aplastó hasta matarlo, veremos que las cosas no siempre salen bien. En el caso de Urada, la investigación reveló que el algoritmo de inteligencia artificial del robot había identificado erróneamente al hombre con un bloqueo del sistema, una amenaza para el funcionamiento de la máquina de la que había que ocuparse de inmediato. El robot estimó que el modo más eficiente de eliminar «la amenaza» era aplastarla con su enorme brazo hidráulico contra la esmeriladora de al lado, una decisión que acabó instantáneamente con la vida de Urada antes de que el robot retomara sin contemplaciones sus tareas habituales. A pesar de los evidentes retos, el incremento exponencial de la productividad, la drástica reducción de costes y el aumento de los beneficios que pueden conseguirse mediante sistemas de inteligencia artificial son tan notables que ya no hay vuelta atrás. La IA ha llegado para quedarse, y Crimen S. A., que nunca deja pasar una oportunidad, se esconde en todos sus rincones.

Al-goritmo Capone y sus *bots* criminales de IA

> Debemos ir con muchísimo cuidado con la IA. Potencialmente, es más peligrosa que la bomba atómica.
>
> ELON MUSK

Como hemos visto en los capítulos anteriores, el uso malicioso de la IA y los algoritmos informáticos ha dado origen a los *bots* criminales: un agente inteligente

programado para perpetrar actividades delictivas a gran escala. Los *bots* criminales constituyen la base de Crimen S. A. y son responsables de su gran incremento de rentabilidad. Estos programas de *software* automatizan los ataques informáticos, la propagación de virus, el robo de propiedad intelectual, el espionaje industrial, el envío de *spam*, la usurpación de identidad y los ataques de denegación de servicio, entre otras amenazas. Los *botnets* informáticos masivos, como Mariposa o Conficker, pueden introducirse en tu ordenador y convertirlo en un poderoso dron de denegación de servicios, y para ello sólo necesitan que uno o dos criminales expertos hayan escrito algoritmos de IA estrecha para conseguirlo.

El *botnet* Gameover Zeus fue capaz de infectar aparatos del todo el mundo con el troyano CryptoLocker, que bloqueaba el acceso de los usuarios a todos sus archivos y los obligaba a pagar si querían recuperarlos. El ataque tuvo éxito gracias a los agentes de *ransomware* inteligentes que Gameover Zeus utilizaba para localizar y destruir los datos de personas inocentes, un delito altamente provechoso que supuso a sus *bots* maestros unas ganancias de unos cien millones de dólares[9]. Llevar a cabo este trabajo de forma manual y con delincuentes humanos habría sido con anterioridad tan prohibitivo como imposible, pero gracias a los avances tecnológicos, Crimen S. A., igual que las aerolíneas, los bancos y las industrias, ha podido incrementar la escala de sus operaciones con una mano de obra enormemente reducida. Es por ello que en la actualidad una sola persona puede robar a otros cien millones; el uso de la IA y los *bots* ha supuesto una escalada exponencial de la delincuencia. Los niveles de automatización delictiva sofisticada que permite la inteligencia artificial, sin parangón con ninguna otra época, son la causa de que las pérdidas anuales atribuidas a los delitos informáticos se hayan disparado hasta alcanzar los más de cuatrocientos mil millones[10].

La IA estrecha proporciona asimismo otro tipo de ayuda a los delincuentes: actúa como un cómplice no humano en sus delitos[11]. En 2012, Pedro Bravo, estudiante de la Universidad de Florida, fue detenido por el presunto asesinato de su compañero de habitación, Christian Aguilar, después de que éste empezara a salir con la exnovia de Bravo. El cuerpo de Aguilar se halló oculto en el bosque, no lejos del campus, y Bravo se convirtió en sospechoso. Tras requerir mediante una orden judicial los registros telefónicos del móvil de Bravo y hacerse finalmente con el dispositivo, la policía realizó dos descubrimientos de gran valor probatorio. En primer lugar, la señal del GPS del supuesto asesino lo ubicaba en el emplazamiento aproximado del cadáver. Por otro lado, y más importante aún, la comprobación de las peticiones a Siri de su iPhone reveló la siguiente frase: «Siri, tengo que esconder a mi compañero de cuarto», a lo que Siri había respondido eficazmente: «Pantanos, embalses, fundiciones de metal y descargas de datos». Tanto la pregunta como la respuesta jugaron un papel determinante en el juicio de Bravo. A medida que mejore la IA, cabe esperar que un número creciente de delincuentes usen estas herramientas como cómplices para que les ayuden a cometer sus delitos. Hemos entrado en la era de Siri

y Clyde.

El pirateo algorítmico también podría ocasionar serios problemas a la sociedad y a sus infraestructuras fundamentales: la mera alteración de unas líneas de códigos entre millones de otras en la programación de un agente inteligente resultaría casi imposible de detectar, pero podría conllevar un cambio drástico en el comportamiento del algoritmo. El ataque contra las centrifugadoras nucleares de las instalaciones de enriquecimiento de uranio de Natanz, en Irán, constituye un ejemplo perfecto de esta clase de amenaza, un cambio sutil que supuso una gran diferencia y que tardaron años en descubrir. ¿Cómo podemos saber si los algoritmos de nuestras operaciones en el mercado bursátil o de nuestros navegadores son erróneos o han sufrido un ataque malicioso? No podemos hasta que ya es demasiado tarde, y ése es un grave problema. El uso y la sofisticación de las oportunidades delictivas que permite la IA estrecha no dejan de aumentar, pero resultan insignificantes en comparación con lo que posibilitarán las formas de inteligencia artificial más potentes, competentes y en rápida evolución en un futuro próximo.

Cuando Watson se lance por el camino del delito

> La inteligencia artificial alcanzará niveles humanos en torno a 2029. Si ampliamos el margen hasta, digamos, 2045, habremos multiplicado la inteligencia, la inteligencia biológica humana de las máquinas de nuestra civilización, por mil millones.
>
> RAY KURZWEIL

En 2011, todos contemplamos con asombro como el superordenador Watson de IBM batía a los campeones mundiales del concurso televisivo de cultura general *Jeopardy!* Mediante el uso de la inteligencia artificial y el procesamiento de lenguajes naturales, Watson asimiló unos doscientos millones de páginas de datos estructurados y desestructurados, que procesó a un ritmo de ochenta teraflops, es decir, ochenta billones de operaciones por segundo. Con ello consiguió vencer cómodamente a Ken Jennings, un concursante de *Jeopardy!* que se había alzado con la victoria en setenta y cuatro programas consecutivos. Jennings se tomó su derrota con deportividad y comentó: «Por mi parte, doy la bienvenida a nuestros nuevos amos, los ordenadores». Es posible que quiera reconsiderar su declaración.

Tan sólo tres años después de batir a Jennings, el superordenador Watson logró una mejora de resultados del 2400 por ciento y redujo sus proporciones en un 90 por ciento, «del tamaño de un dormitorio de matrimonio al de tres cajas de *pizza* apiladas»[12]. Además, Watson ha adoptado un nuevo enfoque en su carrera y utiliza sus vastos poderes cognitivos no para concursos televisivos sino para la medicina. El

MD Anderson Cancer Center utiliza a Watson para ayudar a los médicos a emparejar a los pacientes con los ensayos clínicos, y en el Sloan Kettering Institute, Watson está leyendo con avidez un millón y medio de historiales de pacientes y cientos de miles de artículos de publicaciones oncológicas con el fin de ayudar a los profesionales clínicos a obtener los mejores diagnósticos y tratamientos[13]. IBM ha creado incluso el Watson Business Group, con una inversión prevista de mil millones de dólares, para que empresas, organizaciones sin ánimo de lucro y gobiernos puedan aprovechar las capacidades de Watson. Esta decisión ha puesto la inteligencia artificial del nivel de un superordenador a disposición tanto de pequeñas empresas como de individuos, y es probable que en el futuro también caiga en manos de Crimen S. A. Aunque pueda parecer ridículo sugerir que la delincuencia organizada vaya a utilizar superordenadores dotados de IA con finalidades ilícitas, debemos recordar detenidamente todas las veces que aquél ha hecho un mal uso de la tecnología, pues en este caso el pasado es tan sólo el prólogo. Así pues, debemos estar preparados y preguntarnos qué ocurrirá cuando Watson se lance por el camino del delito. ¿Cuánto dinero blanqueará, cuántas identidades robará, cuántos fraudes fiscales cometerá Watson?

Aunque Watson constituye un ejemplo de una IA estrecha sumamente impresionante, en el futuro sus capacidades seguirán aumentando de forma exponencial, y el resultado será una inteligencia que se acerque o mejore la humana. Algún día la IA podría ocupar incluso el lugar de un capo de la mafia y utilizar sus aptitudes para vender drogas, manejar redes de prostitución, distribuir pornografía infantil e imprimir y expedir armas en 3D. «Don Watson» podría incluso convertirse en un sicario geolocalizando objetivos humanos y pirateando objetos conectados a la Internet de las Cosas que rodean a sus víctimas, como coches, ascensores o robots, con el fin de provocar accidentes cuyo resultado sea la muerte de sus presas. Aunque tales actividades se hallen en el nivel extremo de lo que puede llevar a cabo la IA estrecha, resultarían sencillas para la próxima generación informática: la inteligencia general artificial.

El último invento del hombre: la inteligencia general artificial

> Para cuando Skynet cobró conciencia de sí misma, ya se había propagado por millones de servidores informáticos en todo el mundo. Ordenadores personales en edificios de oficinas, en dormitorios, en todas partes. Era *software* en el ciberespacio. No existía un núcleo del sistema. No podía desconectarse.
>
> JOHN CONNOR,
> *Terminator 3. La rebelión de las máquinas*

Ray Kurzweil ha popularizado la idea de singularidad tecnológica, ese momento futuro en que la inteligencia no humana sobrepasará la inteligencia humana por primera vez en la historia, un cambio tan profundo que a menudo se habla de él en términos de nuestra «invención final»[14].

Aunque muchos puedan considerar disparatada esta idea, en el pasado hemos escuchado predicciones negativas defendidas con la misma firmeza:

- No existe razón alguna para que alguien pueda desear tener un ordenador en su casa (Ken Olsen, presidente de Digital Equipment Corporation, 1977).
- Un cohete jamás podrá ir más allá de la atmósfera terrestre (*New York Times*, 1936).
- Es imposible que existan artefactos voladores más pesados que el aire (lord Kelvin, matemático y físico británico, presidente de la Royal Society, 1895).
- Este «teléfono» tiene demasiadas limitaciones para ser considerado seriamente como un medio de comunicación. El artefacto carece intrínsecamente de cualquier utilidad para nosotros (circular interna de Western Union, 1878).

De algún modo, lo imposible parece convertirse siempre en posible. En el mundo de la inteligencia artificial, esa nueva fase de desarrollo se denomina inteligencia general artificial (IGA), o IA fuerte. A diferencia de la IA débil, que realiza con habilidad una tarea específica limitada, como la traducción automática o la navegación para coches, la IA fuerte hace referencia a «máquinas pensantes» que pueden llevar a cabo las mismas tareas intelectuales que un ser humano. Entre las características de la IA fuerte se incluyen la capacidad de razonar, emitir juicios, planificar, aprender, comunicar y unificar todas esas habilidades con el fin de alcanzar metas comunes en una gran variedad de ámbitos, de modo que el interés comercial por ella no hace más que aumentar. En 2014, Google adquirió DeepMind Technologies por más que quinientos millones de dólares con el fin de fortalecer sus capacidades de aprendizaje profundo de IA, que ya eran potentes de por sí[15]. En la misma línea, Facebook creó un nuevo departamento interno centrado específicamente en IA avanzada. Los optimistas creen que la aparición de la IGA puede traer consigo un período de abundancia sin precedentes en la historia humana, que erradicará las guerras, curará todas las enfermedades, alargará de manera radical la vida humana y terminará con la pobreza. Pero no todo el mundo celebra del mismo modo su posible llegada.

El IA-pocalipsis

Sé que Frank y tú estáis pensando en desconectarme, y me temo que eso es algo

que no puedo permitir.

HAL 9000, en *2001. Una odisea del espacio*

En un artículo de opinión publicado en 2014 en el periódico británico *Independent*, el famoso físico teórico Stephen Hawking realizó una seria advertencia acerca del futuro de la IGA: «Mientras que el efecto a corto plazo de la IA depende de quién la controla, el efecto a largo plazo depende de si es posible controlarla»[16]. Y a continuación declaró que desestimar las máquinas hiperinteligentes por considerarlas «pura ciencia ficción sería un error, y potencialmente el peor error que podríamos cometer», y que lo que teníamos que hacer era esforzarnos más por mejorar nuestras posibilidades de aprovechar los beneficios de la IA al tiempo que minimizamos sus riesgos. En *2001. Una odisea del espacio*, el clásico de ciencia ficción de Stanley Kubrick, el ordenador de a bordo de la nave especial, HAL 9000, se enfrenta a un complicado dilema. Su programación algorítmica le obliga a completar la misión cerca de Júpiter, pero debido a cuestiones de seguridad nacional no puede revelar a la tripulación el objetivo del viaje. Para resolver la contradicción de su programa, intentar matar a la tripulación. A medida que la IA aumenta su potencia, los robots se vuelven más autónomos y, con la IGA acechando en el horizonte, debemos asegurarnos de que los algoritmos del futuro estén mejor equipados para resolver conflictos de programación y dilemas morales de lo que estaba HAL.

No se trata de que una IA fuerte sea necesariamente «malvada» y trate de destruir a la humanidad, pero en su intento de lograr su objetivo primordial tal como está programado, una IGA podría no detenerse hasta haber cumplido su misión a cualquier precio, incluso si eso significara competir con seres humanos o herirlos, apoderarse de nuestros recursos o provocar daños en el medio ambiente. En la medida en que los riesgos percibidos de la IGA han aumentado, se han creado numerosas instituciones sin ánimo de lucro que se dedican a encauzarlos y estudiarlos, como el Future of Humanity Institute de Oxford, el Machine Intelligence Research Institute, el Future of Life Institute y el Cambridge Centre for the Study of Existential Risk.

A pesar de los riesgos señalados por Hawking y otros, la investigación y el desarrollo en el campo de la inteligencia artificial no se han interrumpido. Hay quien piensa incluso que sería posible utilizar la inteligencia artificial para reproducir el neocórtex del cerebro humano. Una de esas empresas, Vicarious, una *start-up* de Silicon Valley, está desarrollando un *software* de IA «basado en los principios de cálculo del cerebro humano». Una IA capaz de aprender. La empresa ha recibido decenas de millones de dólares procedentes de fondos de capital riesgo, incluidas notables inversiones de Mark Zuckerberg, el dueño de Facebook, y del cofundador de PayPal, Peter Thiel[17]. El objetivo de la empresa es recrear la «parte del cerebro que ve, controla el cuerpo, razona y entiende el lenguaje». En otras palabras, Vicarious trata de traducir el neocórtex humano a un código informático, y no está sola en su intención de construir una mente.

Cómo construir un cerebro

> Una neurona típica establece cerca de diez mil conexiones con las neuronas contiguas. Dado que tenemos miles de millones de neuronas, eso significa que en un centímetro cúbico de tejido cerebral hay tantas conexiones como estrellas en la Vía Láctea.
>
> DAVID EAGLEMAN

En abril de 2013, el presidente Obama anunció la creación del Brain Activity Map Project, un plan que llevaba en marcha diez años y cuyo objetivo era cartografiar todas las neuronas del cerebro humano y revolucionar nuestra comprensión para tratar, curar y prevenir los trastornos cerebrales, así como para averiguar con exactitud cómo nuestra mente registra, procesa, utiliza, almacena y recupera enormes cantidades de datos, a la velocidad del pensamiento[18]. Por supuesto, comprender cómo funciona el cerebro sería un primer requisito imprescindible para crear una mente artificial de silicio a semejanza de la humana. El mero hecho de construir un ordenador capaz de hacer funcionar el *software* requerido para simular un cerebro humano es de por sí una tarea hercúlea. Haría falta una máquina con una «capacidad computacional de por lo menos 36,8 petaflops [un petaflop equivale a mil billones de operaciones por segundo] y una capacidad de memoria de 3,2 petabytes». Aunque hace tan sólo unos años no existía una máquina semejante, cabe la posibilidad de que su creación sea inminente[19].

A pesar de lo inverosímil que pueda resultar la idea, destacados científicos y tecnólogos como Ray Kurzweil y Michio Kaku han escrito convincentes obras basadas en investigaciones sobre el tema que subrayan la avanzada tasa de progreso en el campo de la neurociencia[20]. Si bien en general se ha desechado la idea de construir una máquina enormemente inteligente con capacidades al nivel del cerebro humano, y aunque siguen existiendo profundos huecos en nuestro conocimiento del funcionamiento de éste, los fascinantes descubrimientos en el campo de la ciencia del cerebro constituyen un fenómeno creciente[21]. En condiciones de laboratorio, ya se ha logrado registrar los recuerdos de una persona, entablar comunicación telepática, grabar sueños en vídeo y llevar a cabo telequinesia, y nuevos descubrimientos emergen sin parar[22]. En agosto de 2014, el director científico de IBM, Dharmendra Modha, anunció el desarrollo de True North, «un chip de procesamiento neuromórfico inspirado en el cerebro» que IBM pretendía que emulara la arquitectura neurológica del sistema nervioso humano[23]. El chip tiene un número de neuronas programables sin precedentes, un millón, y 256 millones de sinapsis, y la revista *Science* lo definió como «un paso fundamental para acercar la computación cognitiva a la sociedad»[24]. Tal vez uno de los logros más significativos de conseguir lo que teóricamente es una ingeniería inversa del cerebro y crear una arquitectura computarizada capaz de emular la cognición sería la capacidad de analizar el cerebro

para descargarlo tanto a él como a su contenido[25].

Dados los progresos en IA, que avanzan hacia la IGA, si en algún momento es posible recrear la mente humana a través de la computarización cognitiva ello conllevará una gran ventaja para los seres humanos: no habrá límites para el tamaño de su cerebro. Mientras que la capacidad intelectual del *Homo sapiens* se ve limitada por aquello que cabe dentro del cráneo, dicha restricción no sería relevante en el caso de una inteligencia artificial que podría tener un cerebro de cualquier tamaño, otra razón por la que algunos creen que la inteligencia artificial sobrehumana es tal vez nuestro destino.

Aprovechando el genio: interfaz cerebro-ordenador

> Lo que tenemos encima de los hombros es el objeto más complejo del universo conocido.
>
> MICHIO KAKU

Tal vez nos falte mucho para ser capaces de crear una mente humana, pero lo cierto es que se han realizado espectaculares avances en la interacción entre nuestros cerebros de carne y hueso de toda la vida y una amplia variedad de dispositivos informáticos digitales, en el marco de un campo de la ciencia conocido como interfaz cerebro-ordenador (BCI en sus siglas en inglés). La BCI mide y evalúa la actividad eléctrica cerebral, igual que se haría con un EEG, y eso permite una vía de comunicación directa entre el cerebro y un dispositivo informático, que puede estar implantado internamente o llevarse en el exterior. En la actualidad también disponemos de un gran número de neuroprótesis, dispositivos informáticos que «restauran o complementan las capacidades de la mente mediante componentes electrónicos insertados directamente en el sistema nervioso»[26]. El más común de estos dispositivos es el implante coclear, un audífono colocado en el cráneo que se conecta mediante un cable con el nervio auditivo del cerebro, lo cual restablece la capacidad auditiva de las personas que padecen sordera profunda. Las prótesis de retina devuelven parcialmente la visión a los invidentes utilizando diminutas cámaras de vídeo montadas de forma externa que procesan las imágenes y envían los resultados directamente al nervio óptico a través de electrodos. Las pacientes de Parkinson utilizan de manera habitual implantes protésicos neuronales que transmiten impulsos eléctricos al centro del cerebro como medio de minimizar los temblores y restablecer el control motor.

Por sorprendente que resulte todo ello, se trata tan sólo del comienzo de lo que la BCI hace posible. Ya sea con un implante neuronal o mediante unos auriculares EEG externos con sensores colocados en el cuero cabelludo, es posible conseguir que un

software procese nuestras ondas cerebrales hasta el punto de poder controlar objetos físicos por el mero hecho de pensar en la acción deseada, sin necesidad de mover un dedo. Jan Scheuermann, una mujer tetrapléjica que no puede mover sus extremidades debido a una degeneración espinal, ha podido utilizar su mente para controlar un brazo robótico externo y comer ella sola por primera vez en una década gracias a la tecnología[27].

Existen incluso elegantes auriculares EEG para el público general, como el Emotiv o el NeuroSky, que por menos de trescientos dólares permiten controlar con la mente desde videojuegos hasta objetos físicos que pueden moverse a nuestro alrededor, incluidos robots[28]. Una empresa británica ha unido recientemente el biosensor EEG de NeuroSky con las Google Glass utilizando una aplicación de Android que han desarrollado, llamada MindRDR, que controla las gafas con el pensamiento, una evolución que permite tomar una fotografía tan sólo pensando en ello[29]. El nuevo y pujante movimiento OpenBCI (*software* libre de interfaz cerebroordenador) garantizará que en el futuro sigan desarrollándose en este ámbito nuevas oleadas de logros científicos a bajo coste. Un grupo de investigadores de la Universidad de Washington ha creado con éxito la primera «interfaz no invasiva entre cerebros por Internet». Equipado con un casco de estimulación magnética transcraneal, un investigador fue capaz de «controlar de forma remota la mano de otro a través de Internet, limitándose a pensar en mover la mano»[30]. Para que los dispositivos BCI funcionen, es necesario que nuestras ondas cerebrales se transformen en instrucciones que un ordenador pueda comprender, y las repuestas digitales del ordenador deben transmutarse de nuevo en ondas cerebrales para que nuestras mentes puedan procesarlas. Pero si un robot, un videojuego o una prótesis neuronal puede leer tu mente, ¿quién más puede hacerlo?

Leer la mente, certificados cerebrales y neuropiratas

Ciertas tecnologías nos permiten introducirnos más y más en el funcionamiento de la mente humana, en particular la imagen por resonancia magnética funcional (IRMf), una prueba no invasiva que utiliza potentes campos magnéticos y ondas de radio para elaborar un mapa del cerebro y calibrar los cambios en el flujo sanguíneo para medir la actividad cerebral. En un revolucionario experimento llevado a cabo en la UC Berkley, la IRMf permitió a los neurocientíficos reconstruir los rostros que estaba mirando un grupo de personas basándose tan sólo en su actividad cerebral y lo que veían mentalmente[31]. En la Universidad Carnegie Mellon, por su parte, los investigadores utilizaron la IRMf para llevar a cabo de forma correcta y repetida «identificaciones mentales», es decir, identificar el objeto en el que pensaba una

persona, como un martillo o un cuchillo, analizando tan sólo su escáner cerebral[32]. Estos y otros estudios llevaron a IBM a pronosticar que en 2017 la existencia de formas parciales de leer la mente ya no sería cosa de ciencia ficción[33].

En la actualidad ya se han creado varias empresas comerciales con el fin de aprovechar las oportunidades de negocio que permite la «identificación mental», entre ellas dos que se centran en el uso de la IRMf para detectar mentiras: No Lie MRI y Cephos[34]. Sus pruebas están corroboradas por Joshua Green, profesor de Harvard cuyas investigaciones sugieren que la corteza prefrontal se muestra más activa en aquellas personas que están mintiendo, una información que resulta muy útil a la policía[35]. Mientras los expertos en neuroética ponderan las consecuencias de todo esto, cuerpos de seguridad de todo el mundo intentan ya utilizar los resultados de los escáneres cerebrales en los procedimientos penales. En India, una mujer fue condenada por el asesinato con arsénico de su exprometido después de que su escáner cerebral «probara» que tenía conocimiento empírico de haber cometido el crimen[36]. En los juzgados estadounidenses, conforme a la Quinta Enmienda, no se puede obligar a un acusado a declarar en su contra, pero ¿cómo se concilia eso con la tecnología IRMf? En la actualidad, sí puede exigirse al acusado que proporcione muestras de ADN o de sangre, así que, ¿por qué no «muestras cerebrales»? A medida que mejora la tecnología, sin duda cabe esperar un incremento de peticiones de «certificados cerebrales» mientras el juez llama al siguiente testigo, tu mente, para que testifique en tu contra.

Está claro que si médicos, científicos y policías tienen acceso a una tecnología, Crimen S. A. no les va a la zaga y seguro que siente curiosidad por saber lo que piensas. Lo primero que cabe esperar es que los piratas empiecen por atacar las neuroprótesis, tal como hicieron con otros dispositivos médicos implantables, como marcapasos y bombas de insulina, tratando de sabotear sus comunicaciones y los protocolos de control. Por ejemplo, un atacante podría apagar los electrodos estabilizadores de un estimulador cerebral profundo de un paciente de Parkinson, lo cual conllevaría la reanudación de los intensos temblores o una crisis epiléptica. Por otra parte, si dos investigadores de la Universidad de Washington pueden comunicarse telepáticamente e incluso mandar señales de estimulación motora muscular a través de Internet de modo que una persona mueva de manera involuntaria una parte de su cuerpo mediante el mero pensamiento, ¿qué impediría a un tercero con malas intenciones piratear dicho sistema y hacer lo mismo? Mientras tú utilizas tu sofisticado biosensor EEG para jugar a Pong, mover objetos en la Internet de las Cosas, controlar tu dron cuadricóptero y tomar una fotografía con tus Google Glass mediante el impresionante poder de tu mente, ¿qué podría impedir que un tercero se conectase de manera remota e hiciera lo mismo? Como hemos visto una y otra vez en este libro, absolutamente nada. De hecho, es posible que ya esté sucediendo. En 2012, investigadores de la Universidad de Oxford, la UC Berkeley y la Universidad de Ginebra demostraron que era posible lanzar un ataque contra los usuarios de

auriculares EEG como el Emotiv para robar información personal sensible[37]. Mientras los sujetos del estudio llevaban los auriculares puestos, los investigadores les mostraban brevemente imágenes de cosas como teclados de cajeros automáticos para introducir el PIN, tarjetas de crédito y calendarios. Debajo de las imágenes subyacían preguntas como ¿cuál es tu pin? o ¿cuál es tu fecha de nacimiento? Los resultados fueron impactantes: al leer las ondas cerebrales que irradiaban de estos auriculares de trescientos dólares, los investigadores fueron capaces de averiguar el PIN de los sujetos con un 30 por ciento de fiabilidad y la fecha de nacimiento con un 60 por ciento. Los resultados son significativos en la medida en que se obtuvieron con dispositivos EEG de biofeedback al alcance del consumidor medio y cada vez más populares (no con máquinas de IRMf). Tanto Emotiv como NeuroSky disponen de app stores en las que los usuarios pueden descargarse aplicaciones de terceros, igual que hacemos en nuestros móviles. Y dada la furia con la que Crimen S. A. ha atacado las tiendas de aplicaciones telefónicas y las ha sembrado de *software* malicioso y aplicaciones fraudulentas, ¿cuánto tiempo pasará antes de que suba «spyware cerebral» a estos nuevos mercados online? Aunque como veremos, tus células cerebrales no son la única parte de tu biología que podría estar amenazada.

La biología es una tecnología de la información

> Ha llegado el momento de despedirse del siglo de la física, aquél en el que dividimos el átomo y convertimos el silicio en poder de computación. Es hora de dar la bienvenida al siglo de la biotecnología.
>
> WALTER ISAACSON, *Time*, 22 de marzo de 1999

A lo largo de este libro, hemos centrado nuestra atención en tecnologías basadas en el silicio: microchips, teléfonos inteligentes, robótica, datos masivos, monedas digitales y realidad virtual, por nombrar sólo unas cuantas. Estas herramientas hablan el idioma de los unos y los ceros, la lengua materna del código binario que entienden todos los aparatos digitales. Pero existe otro sistema operativo, uno mucho más generalizado que Windows, UNIX o Mac. Desde las algas a las orquídeas pasando por los orangutanes, este sistema operativo lo utiliza tanto la fauna como la flora. Se trata del ADN, el sistema operativo original del mundo, y durante la mayor parte de la historia de la humanidad ni siquiera sabíamos que existía.

El sorprendente descubrimiento en 1953 por parte de Watson y *Crick* de la estructura molecular del ácido desoxirribonucleico con sus cuatro letras del alfabeto genético —A (adenina), C (citosina), G (guanina) y T (timina)— cambió por completo el paradigma. Pero debido a los costes y limitaciones de la potencia del procesamiento informático, hasta abril de 2013 el Proyecto Genoma Humano (con la

ayuda del empresario J. Craig Venter) no pudo transformar las aes, tes, ces y ges, el código compartido por todas las formas de vida del planeta, en los unos y ceros que los ordenadores de silicio podían entender. La genómica, la base de toda vida biológica, se había convertido en una tecnología de la información. Desde entonces no han dejado de aparecer nuevos dispositivos, cada uno de los cuales rebaja el coste de la secuenciación del ADN, de modo que el gasto medio se reduce a la mitad cada dieciocho meses más o menos. Esta proporción se ajusta a ley de Moore, lo que a su vez produjo mejores ordenadores para procesar todos estos datos genéticos. El coste de secuenciar un genoma humano completo cayó con rapidez de unos tres mil millones de dólares en 2010 a un millón en 2006 y cien mil dólares en 2008[38]. Fue precisamente en 2008 cuando sucedió algo sorprendente: la creación de los denominados secuenciadores de nueva generación provocó la caída en picado del precio de la decodificación del genoma humano. Como resultado, los avances en la secuenciación genética superaron en cinco los avances informáticos[39]. En 2014 habíamos entrado en la era del mapa completo del genoma humano por mil dólares. Empresas como 23andMe ofrecían pruebas de ADN caseras para el público general por 99 dólares o menos; sólo era necesario escupir en un tubo de plástico, enviarlo en un sobre con el franqueo pagado y al cabo de una semana o dos se podían consultar en línea los resultados sobre la salud, la ascendencia y la genealogía.

De cara al futuro, la evolución de la secuenciación del ADN sugiere que dentro de unos años su coste se reducirá hasta el punto de que alguna empresa pagará para secuenciar a sus nuevos clientes, no ya por poco dinero sino gratis, un modelo de negocio ampliamente utilizado en la tecnología informática. Cuando esto ocurra, cada uno de nosotros (y muchas empresas) tendremos la oportunidad de conocer nuestra dotación genética completa, una novedad con implicaciones radicales para la medicina y para nuestro sistema sanitario[40]. Esta caída drástica de los costes no se produce sólo en el ámbito de la lectura del ADN, sino también en la tecnología que permite escribirlo[41]. Desde comienzos del milenio, el precio de la síntesis química del ADN ha mejorado a un ritmo exponencial, desde los veinte dólares por base de 2000 hasta los veinte céntimos por base en 2014, al tiempo que se ha incrementado la extensión del código de ADN que puede escribirse (equivalente aproximadamente a la complejidad del programa genético). En la medida en que la escritura del código del ADN constituye la base de la ingeniería genética, los científicos actuales pueden hacer mucho más y más rápido que los ingenieros genéticos del pasado, que tenían que manipular la molécula de ADN físicamente (en oposición a la manipulación digital contemporánea). Este campo emergente se conoce como biología sintética.

La biología sintética es la ingeniería de la biología, desde células individuales hasta organismos enteros, y nos permite rediseñar sistemas biológicos existentes o crear otros completamente nuevos. Si la secuenciación del genoma consiste en leer los pares de bases del ADN convirtiéndolos en ceros y unos en la pantalla de un ordenador, la biología sintética es en esencia el proceso inverso: diseñar material

genético en código informático binario y traducirlo a secuencias de ADN que pueden crearse en el mundo real. La ingeniería genética se vuelve así tan sencilla como la ingeniería de *software*. Como explica el biólogo sintético Andrew Hessel, «las células son como ordenadores en miniatura y el ADN es su *software*, que les da instrucciones sobre las funciones que deben llevar a cabo». En la actualidad existen docenas de tiendas de impresión de ADN, una especie de Kinko biológico, que pueden convertir un diseño digital en ADN mediante la impresión en 3D de la molécula de ADN. También existen biomercados de impresión online donde uno puede subir sus diseños biológicos digitales y recibir a través de FedEx un vial con el ADN encargado. Asimismo, es posible contratar los servicios de *fab labs* más sofisticados capaces de diseñar y crear un organismo entero.

No cabe duda de que esta drástica reducción del precio ha democratizado la ciencia biológica y la genética, y ha estimulado la aparición de un movimiento de «bioaficionados» al permitir a ciudadanos científicos y biólogos aficionados experimentar con la biología sintética en sus propias casas y garajes, lo cual ha supuesto enormes innovaciones en este campo. Venter se ha atrevido a pronosticar que «durante los próximos veinte años, la genómica sintética será algo habitual para hacer cualquier cosa»[42], una previsión totalmente posible si tenemos en cuenta que la biología moderna se ha convertido en una rama de la tecnología de la información.

Bioordenadores y discos duros de ADN

> Si hoy fuera adolescente, me dedicaría a piratear la biología.
>
> BILL GATES

La integración entre la biología y la tecnología de la información ha llegado a tal extremo en los últimos años que los científicos han podido crear bioordenadores reales, utilizando ADN y proteínas para llevar a cabo cálculos relacionados con el almacenamiento, la recuperación y el procesamiento de datos[43]. El emergente campo del bioalmacenamiento se vale de la biología sintética para codificar datos de los seres vivos a través del código de su ADN, tomando los unos y los ceros de nuestros ordenadores digitales y transformándolos en las ATCG del código genético para implantarlas en el ADN[44]. Así pues, es posible codificar y almacenar textos, imágenes, música y videos dentro de las células, y la eficacia de este método es impresionante. El conocido genetista, ingeniero molecular y profesor de Harvard George Church ha concluido que «hipotéticamente, unos cuatro gramos de ADN podrían almacenar todos los datos digitales que la humanidad genera en un año»[45].

Estas técnicas de almacenamiento no sólo superan ampliamente en longevidad a

los medios magnéticos por unos cuantos cientos de miles de años (hoy en día aún podemos leer el ADN de los dinosaurios), sino que además son más de un millón de veces más densas que las actuales técnicas de almacenamiento electrónicas[46]. Joi Ito, del Media Lab del MIT, ha pronosticado que, como resultado, nuestro universo tecnológico se expandirá más allá de la Internet de las Cosas hasta incluir una Internet de los microbios, redes de cosas biológicas que pueden comunicarse entre ellas y con nosotros. No cabe duda de que la biología sintética augura numerosos avances y beneficios para nuestra sociedad, y el trabajo tan sólo acaba de empezar.

La capacidad de reprogramar el ADN y de construir biología supone una enorme promesa para que la humanidad pueda solucionar algunos de los problemas más complejos del mundo en el campo de la medicina, la agricultura, la energía y el medio ambiente. El impacto de la biología sintética en la sanidad contribuirá a revolucionar la prevención, el diagnóstico y el tratamiento de las enfermedades. Equipados con nuestras propias secuencias genéticas, podremos recibir tratamientos médicos hechos a medida, medicamentos diseñados específicamente para nuestra dotación genética única. Se trata de algo que ya puede observarse en el ámbito de la oncología, en el que es posible obtener un genotipo de los tumores individuales y crear tratamientos personalizados para destruir células cancerígenas concretas sin dañar las células sanas de alrededor. De hecho, la biología sintética permitirá un gran número de terapias, como nuevas vacunas, avances en la medicina regenerativa, un tratamiento para la malaria e incluso la cura para la sordera congénita[47]. Pero este nuevo poder divino para crear conlleva una responsabilidad igual de grande.

Un parque jurásico real

Aunque los niños que acuden al Museo Americano de Historia Natural de Nueva York pueden contemplar el esqueleto expuesto de un lanudo mamut extinguido hace tiempo, tienen que echar mano de la imaginación para visualizar el aspecto que tendría el animal en la época en que caminaba sobre la Tierra. Dentro de poco ya no tendrán que imaginarlo, pues podrán verlo en el zoo del Bronx. Los expertos en paleogenómica están trabajando en la extracción de ADN de un colmillo de mamut de veinte mil años de antigüedad hallado a principios de 2014 en una zona en obras de Seattle. Para ello utilizan técnicas genéticas avanzadas que les permitan aislar el ADN, clonarlo e implantarlo en un embrión que crecerá en el vientre de una elefanta africana.

Al mamut extinguido podrían unírsele a no mucho tardar el dodo, la paloma pasajera y el tigre de Tasmania, especies que pueden reintroducirse en la actualidad gracias a un proceso controvertido conocido como desextinción[48]. Reintroducir

animales extinguidos podría reportar beneficios y sin duda plantea muchas controversias, pero el verdadero poder de la biología sintética se refleja en el hecho de que también podemos crear de la nada especies completamente nuevas, cosa que ya se ha hecho. En 2010, Craig Venter creó la «primera forma de vida sintética que ha existido nunca en el planeta, una especie celular autorreplicable cuyo padre era un ordenador». En otro ejemplo de creación de organismos, una empresa llamada Growing Plant se dedica a dotar a las plantas normales de «bioluminiscencia», es decir, hacer que brillen en la oscuridad[49]. Mediante el uso de patrones de ADN libres y de código abierto, la idea de la empresa es proporcionar «iluminación natural sin electricidad», de modo que algún día las farolas de tu calle serán sustituidas por árboles que brillarán en la oscuridad cuando el sol se ponga. Estamos hablando de una evolución a gran escala. Pero por genial y formidable que parezca, encierra peligros desconocidos.

La invasión de los ladrones biológicos: privacidad genética, bioética y acosadores de ADN

La película de 1997 *Gattaca* se desarrolla en el futuro cercano y retrata un mundo en el que los ricos conciben a sus hijos mediante la eugenesia, una manipulación genética que garantiza que los ciudadanos posean tan sólo «los mejores» rasgos genéticos. Aquellos que nacen fuera del sistema se enfrentan a una vida de discriminación genética con oportunidades laborales limitadas. Se pretendía que fuera una película de ciencia ficción, pero tal vez ya no lo sea. Nuestro ADN, nuestras células y otros datos biológicos pueden ser recopilados para utilizarlos de formas que la mayoría de nosotros jamás habría imaginado. Tal vez el caso más tristemente célebre sea el de Henrietta Lacks, una afroamericana pobre del sur de Estados Unidos cuyo tumor cancerígeno le sobrevivió mucho tiempo después de su muerte en 1951. Las células cancerígenas de Lacks tenían una propiedad que no se había visto nunca antes: la capacidad única de mantenerse con vida y crecer fuera del cuerpo. El descubrimiento tuvo enormes repercusiones en la investigación médica, y sus células inmortales, que acabaron por conocerse como «línea HeLa», fueron enviadas a todo el mundo y se usaron repetidamente en la investigación para tratar la polio y luchar contra el cáncer y el sida. Desde la muerte de Lacks, los científicos han cultivados veinte toneladas de sus células y han comerciado con ellas, aunque ni ella ni su familia dieron nunca su autorización. Finalmente sus herederos demandaron a la Universidad de California, que utilizaba las células para sus investigaciones, pero el Tribunal Supremo del estado dictaminó que «los tejidos y células desechados de un persona no son propiedad suya y puede comerciarse con ellos»[50]. Recuérdalo la

próxima vez que vayas al médico.

Igual que Lacks, todos compartimos material genético todo el tiempo, nos demos cuenta o no. No dejamos el rastro de nuestro ADN sólo cuando acudimos al médico para un análisis de sangre rutinario, sino también en cada cepillo que usamos para peinarnos, en el cepillo con el que nos lavamos los dientes y en cada vaso del que bebemos un sorbo de agua. Como la Internet de las Cosas (y de los microbios) funciona en línea, los miles de millones de células cutáneas que se desprenden a diario de nuestro cuerpo acabarán por ser detectadas mediante sensores en la entrada de los centros comerciales, en los aeropuertos, en las tiendas y por toda la ciudad, lo que nos convertirá en extraordinariamente rastreables de una forma que un teléfono móvil no permite. Este ADN puede ser recuperado, replicado y secuenciado a voluntad por cualquiera que lo desee y tenga los medios para hacerlo, y en la medida en que el coste de la secuenciación genética tiende a cero, se trata de una preocupación creciente a la que debemos enfrentarnos. El genoma completo de Henrietta Lack fue finalmente publicado en Internet en 2013 por un científico alemán, de nuevo sin el consentimiento de sus familiares. ¿Por qué debería preocuparles, tanto a ellos como a nosotros[51]? Porque nuestro material genético revela más sobre nosotros que cualquier cuenta en línea pirateada, y porque nuestro ADN puede utilizarse no sólo para proporcionarnos un tratamiento médico sino también para hacernos daño.

Nuestra dotación genética también cuenta historias que tal vez no queramos compartir con los demás, como nuestra predisposición psicológica a la obesidad, el alcoholismo, la agresividad, las enfermedades cardiovasculares, la depresión, la esquizofrenia, la diabetes, los trastornos bipolares, el TDAH y el cáncer de mama[52]. Algunos estudios han establecido también vínculos de diversa intensidad entre el ADN y la orientación sexual, las tendencias impulsivas e incluso la criminalidad[53]. En ésta distopía futura inspirada en *Gattaca*, toda esta información podrá y será usada contra ti. *Soy el dueño de un pequeño negocio; ¿por qué contratar a una mujer con predisposición a padecer cáncer de mama? El precio de mi seguro médico se dispararía. Quiero un niño «normal»; a lo mejor debería abortar el feto gay que lleva mi mujer en el vientre. Claro que cometió la violación; su ADN demostró que era hiperagresivo y tenía problemas para controlar sus impulsos*.

En Estados Unidos existen pocas leyes que protejan el uso que puede darse a esta clase de información, con la excepción de la GINA (ley de no discriminación por información genética de 2008, en sus siglas en inglés), que declara ilegal que los empleadores contraten o rechacen a un candidato en base a información genética. Aunque la GINA se aplica para los seguros médicos, no protege contra el uso por parte de las compañías de seguros de información obtenida con pruebas genéticas para discriminar en el momento de redactar las pólizas de los seguros de vida, por incapacidad o de asistencia de larga duración[54]. Diversas personas, entre ellas Pamela Fink, de Connecticut, han declarado que fueron despedidas porque sus

empleadores averiguaron que eran portadoras del gen BRCA2, que las predispone a padecer cáncer de mama, un caso que se resolvió extrajudicialmente mediante un acuerdo[55].

Mientras tanto, en base a la ley danesa, todos los niños de ese país nacidos desde 1981 han sido objeto de análisis genéticos obligatorios y sus muestras se almacenan a perpetuidad, muestras recogidas supuestamente por razones de salud pública pero que desde entonces se han utilizado para identificar a numerosos delincuentes[56]. ¿Qué más podría hacer el gobierno danés o cualquier otro con estos datos? ¿Podría el ADN almacenado en una base de datos nacional convertirse en la próxima Henrietta Lacks? Y ¿qué ocurre cuando al final estos datos genéticos se filtran y acaban siendo de dominio público, como ocurrió con la base nacional de datos biométricos israelí, robada por piratas informáticos y reposteada a lo largo y ancho de la clandestinidad digital[57]? Estas posibilidades resultan preocupantes sobre todo porque los científicos israelíes han demostrado que es posible fabricar evidencias genéticas basándose sólo en el perfil de ADN almacenado en una base de datos, sin necesidad de disponer de una muestra de tejido del individuo concreto. Eso significa que hoy en día es posible colocar la sangre o la saliva de una persona inocente en el escenario de un crimen. Las muestras creadas eran tan buenas que los laboratorios forenses policiales fueron incapaces de diferenciarlas de las reales así como de detectar cualquier manipulación[58]. Gracias a los avances en biología digital, las pruebas de ADN, que con anterioridad constituían la prueba de referencia en el ámbito de las evidencias forenses, están ahora amenazadas, y cualquiera que tenga interés en ello podría tenderte una trampa de la que te sería imposible escapar. Buena suerte cuando se lo expliques a los policías mientras te detienen.

En la actualidad ni siquiera hace falta ser biólogo sintético para acceder a las herramientas que permiten la secuenciación genética. Empresas como EasyDNA aceptarán alegremente cualquier objeto que les envíes por correo, ya sea un chicle, una colilla, hilo dental, cuchillas, palillos, sellos chupados o pañuelos de papel usados, lo secuenciarán y lo analizarán para determinar la paternidad o la genealogía de una persona, o el sexo de un bebé, así como para otras cuestiones legales y médicas. Se conocen como «muestras de ADN discretas» y procesar una cuesta unos cien dólares[59]. ¿No estás seguro de contratar a ese chico nuevo que ha venido a tu despacho para realizar una entrevista? Sólo tienes que mandar al laboratorio la taza de café que ha dejado al marcharse para averiguar si constituye un posible riesgo debido a un montón de gravosas enfermedades que podrían costarle un dineral a tu empresa. ¿Odias a tu exnovio? ¿Por qué no colgar en Internet su secuencia genética y demostrar al mundo entero que su ADN mostraba un riesgo elevado de enfermedad mental o alcoholismo? Lo creas o no, coger el ADN de un desconocido y mandarlo a un laboratorio es totalmente legal, y no hay nada que pueda impedirlo aparte de las limitadas excepciones que violan la GINA. Los avances en biología sintética no sólo suscitarán un montón de problemas éticos y de privacidad: también crearán

problemas criminales, una oportunidad que Crimen S. A. está impaciente por aprovechar en su propio beneficio.

Biocárteles y el nuevo opio del pueblo

La delincuencia organizada siempre ha obtenido dinero de las drogas, mucho dinero[60]. En el punto álgido de su reinado, se dice que el colombiano Pablo Escobar ingresaba cada día sesenta millones de dólares en las arcas de su «empresa»[61]. Más recientemente, se estimó que el mexicano Joaquín *El Chapo* Guzmán Loera atesoraba miles de millones, lo que le valió la inclusión en la lista Forbes de los más ricos del mundo. Su ámbito empresarial consistía sobre todo en la agricultura y la logística: cultivar plantas, destilar sus frutos en sustancias que coloquen a la gente y distribuirlas por el mundo. Los cárteles siempre se han apresurado a introducir la tecnología en sus operaciones: en las comunicaciones, la gestión de la cadena de suministros, la contrainteligencia y la fitotecnia. Aunque los narcos han usado la ingeniería genética desde la época de *Corrupción en Miami*, la biología sintética atesora el potencial para alterar por completo la forma en que éstos hacen negocios, en la medida en que ofrece en potencia beneficios infinitamente mayores y redes de distribución mucho más simplificadas y con menos riesgos[62]. La biología sintética no sólo puede usarse para hacer que las plantas brillen y para luchar contra células cancerígenas individuales, sino que también genera fuertes incentivos económicos y oportunidades para que Crimen S. A. fabrique nuevas rutas metabólicas tanto para drogas ilegales como para medicamentos falsificados.

La biología sintética posibilita el paso de un mundo de estupefacientes elaborados con plantas a otro sintético. ¿Para qué se necesitan ya las plantas? Puedes coger los códigos genéticos de los ingredientes activos de la marihuana, la adormidera verde y las hojas de coca, y cortarlos y pegarlos en levadura[63]. A su vez, puede programarse la levadura para que cultive la maría, la morfina, la cocaína y la heroína por ti; una levadura que puede hornearse para hacer pan y fermentarse para obtener cerveza, lo que significa que en el futuro vamos a disfrutar de un pan y una cerveza muy interesantes. La adopción de este método supone ventajas radicalmente innovadoras para los cárteles existentes. Ya no se necesitan miles de hectáreas para cultivar adormideras verdes y coca que pueden detectar con facilidad los equipos de vigilancia aéreos. Ya no hay necesidad de pasar de contrabando por la frontera cargamentos con toneladas de heroína o cocaína fácilmente detectables. Nada que temer tampoco de los perros detectores de droga. Con unos miles de millones de células de levadura por milímetro, un pequeño vial podría replicarse una y otra vez en condiciones controladas y, con eso, Crimen S. A. se abastecería de sobras hasta el

siglo que viene.

Quienes consideren que un futuro semejante es inverosímil sólo tienen que prestar atención a los progresos que ya se han conseguido con la biología sintética y la creación de fármacos. La bacteria *E. coli* ha sido sometida a ingeniería y reprogramación genéticas para obtener THC (la sustancia activa del cannabis), y también se ha conseguido manipular la levadura de panadero para elaborar LSD y opio[64]. Los rápidos progresos en el campo de la biología digital también pueden desintermediar a algunos de los actores actuales del narcotráfico. Del mismo modo que Microsoft le quitó el ordenador personal a IBM y Apple le quitó el teléfono móvil a Nokia y Blackberry, podría ser un estudiante del MIT quien evitara la necesidad de un Pablo Escobar colombiano del futuro. Es más, si Craig Venter está en lo cierto y todos acabaremos por disponer de bioimpresoras en casa, ¿por qué no imprimir mi propio THC u oxicodona? Eso haría que los herederos de los actuales narcotraficantes vieran evaporarse miles de millones de dólares en beneficios y crearía nuevos líderes para los biocárteles del mañana.

Piratear el *software* de la vida: biodelincuencia y bioterrorismo

> A corto plazo, creo que varios de los avances de la biología sintética resultan bastante desconcertantes. Hemos adquirido la capacidad de crear agentes patógenos de diseño, y existen genotipos de varios organismos infecciosos que son accesibles al público: es posible descargar de Internet la secuencia del gen de la viruela o del virus de la gripe de 1918.
>
> NICK BOSTROM

En los años setenta y ochenta del siglo pasado, grupos como el conocido Homebrew Computer Club de Silicon Valley empezaron a reunirse para hablar de tecnología y de piratear con fines beneficiosos. Hoy en día existe un enérgico movimiento de biología HUM que parte en gran medida de las mismas premisas, con laboratorios comunitarios locales como Genspace en Nueva York y BioCurious en California, que proporcionan espacios y herramientas para que los ciudadanos científicos puedan reunirse y compartir conocimientos. Se trata de biopiratas, en el sentido original del término, que piratean para hacer el bien. Aunque el ADN es el sistema operativo original del mundo, para los piratas es tan sólo otro sistema operativo que espera a que alguien descubra sus grietas.

A pesar de que no exista mala intención, los accidentes relacionados con agentes patógenos cultivados en laboratorio pueden resultar mortales. En 1977, la gripe porcina, un patógeno extinguido durante veinte años, reapareció de forma repentina.

Más adelante se descubrió que volvió a penetrar en la población después de que un modesto trabajador de un laboratorio manejara de forma descuidada una muestra que llevaba congelada desde los años cincuenta[65]. Más recientemente han tenido lugar varios bioaccidentes con consecuencias potencialmente letales. En marzo de 2013, funcionarios de un laboratorio de investigación de máxima seguridad de Texas declararon que habían perdido un vial que contenía virus Guanamito, un patógeno que provoca «hemorragias subcutáneas, en órganos internos o a través de orificios corporales como la boca, los ojos o las orejas», y el FBI está investigando el asunto. Tan sólo un año después, en el Instituto Pasteur de París desaparecieron dos mil viales que contenían el virus SARS, biotoxinas que si caían en manos de gobiernos canallas o de terroristas podían utilizarse como armas biológicas[66].

En el pasado ya hemos visto casos de mala utilización de la biología, sobre todo relacionados con tramas de bioterrorismo en las que se han propagado agentes biológicos dañinos. El ejemplo más conocido es el envío de esporas de ántrax a miembros de los medios de comunicación y senadores estadounidenses en 2001, que causó la muerte de cinco personas que habían entrado en contacto con los sobres mortales. En el extranjero, sabemos que Al Qaeda ha intentado construir armas biológicas y sus socios en Yemen han estado trabajando para crear grandes cantidades de ricina, una toxina blanca en polvo tan letal que una sola mota mata al instante[67]. Es sabido que muchas otras organizaciones terroristas también han creado armas biológicas, en especial Aum Shinrikyo, el grupo responsable del ataque de 1995 con gas sarín en el metro de Tokio que mató a trece personas e hirió a casi mil más[68]. Lo que la mayoría de la gente no sabe acerca de ese infame ataque en el metro es que originalmente Aum había planeado un bioataque masivo contra Tokio y durante diez años había gastado cerca de diez millones de dólares en investigación y desarrollo en un intento de crear una potente biotoxina apropiada. Dados los limitados avances en biotecnología de los años ochenta y principios de los noventa, la organización abandonó su búsqueda de un arma biológica en favor de una química. Hoy en día resultaría significativamente más sencillo llevar a cabo un ataque semejante.

Es posible que los terroristas del presente y del futuro ya no tengan que preocuparse por las dificultades para conseguir acceder a los patógenos y agentes biológicos controlados en los laboratorios gubernamentales. Con el surgimiento de la biología sintética, pueden limitarse a descargar la secuencia genética de un genotipo e imprimir ellos mismos estos virus mortales. Los códigos genéticos completos de algunos de los patógenos más letales del mundo, entre ellos el ébola y la gripe española, pueden descargarse libremente en la base de datos de secuencias de ADN del National Center for Biotechnology Information. Como prueba, Eckard Wimmer, un virólogo universitario, consiguió en 2004 sintetizar el genoma de la polio utilizando un ADN solicitado por correo[69]. En aquella época le costó trescientos mil dólares; hoy se habría acercado más a los mil y, en el futuro, costaría menos que un café con leche. Aunque gobiernos de todo el mundo se han gastado miles de millones

tratando de erradicar la polio, un terrorista, un gobierno canalla o un lobo solitario podría reintroducirla mañana por tan sólo unos dólares. La ingeniería genética que en el pasado era extremadamente compleja y cara, puede llevarse a cabo en la actualidad en cualquier lugar con unas semanas de formación, un ordenador portátil y una tarjeta de crédito.

Por supuesto, los futuros biodelincuentes no dependerán de patógenos conocidos o existentes: mediante la biología sintética, podrán crear sus propios virus, todavía más letales. Recientemente hemos visto un ejemplo: en Holanda y Estados Unidos, un grupo de investigadores alteró el código genético de la gripe aviaria (virus H5N1) para aumentar su capacidad letal. Aunque la gripe aviaria tiene una tasa de mortalidad del 70 por ciento, es difícil que los humanos se contagien. Sin embargo, con tan sólo cuatro mutaciones genéticas, el equipo holandés-estadounidense consiguió crear una cepa mucho más virulenta capaz de transmitirse por el aire, lo cual incrementó de forma sustancial su capacidad de contagio a los humanos y la convirtió en una eficaz arma[70]. El objetivo inicial de la investigación era estudiar a qué velocidad podía evolucionar el H5N1, para prevenir mejor su difusión, pero la cepa alterada genéticamente, si se hubiera liberado, podría haber generado de inmediato una pandemia mundial. En nombre de la ciencia, los investigadores quisieron publicar sus resultados, incluido el código genético de la cepa más virulenta que habían creado, en las revistas *Science* y *Nature*, pero muchos argumentaron que eso sería como proporcionar un libro de recetas a los terroristas para que crearan armas biológicas. Al final, por primer vez en la historia, la National Science Advisory Board for Biosecurity intervino y pidió a las publicaciones que limitaran los detalles de los artículos, a lo que éstas accedieron temporalmente[71]. Este riesgo concreto se evitó de manera temporal, pero en último término el código se filtrará y no cabe duda de que se crearán otros.

Aunque un ataque bioterrorista masivo resultaría devastador, la biología sintética permite fijar como objetivo no sólo a una población entera sino también a un individuo en concreto entre millones de otros. La medicina personalizada ha demostrado que es posible actuar sobre una célula individual al tiempo que se dejan intactas las que la rodean, pero el reverso de la moneda son las armas biológicas personalizadas. En el futuro, a los aspirantes a bioasesinos sólo les hará falta recuperar material genético del tenedor o la cuchara de un restaurante, tal vez de un político prominente o de un famoso, para crear un virus destructivo a medida[72]. Aunque alguien podría creer que dicha situación pertenece al reino de la ciencia ficción, el escándalo de WikiLeaks reveló que supuestamente el gobierno de Estados Unidos había enviado telegramas diplomáticos a sus embajadas del otro lado del Atlántico instruyendo a su personal para que tratara de recoger el ADN de líderes mundiales, es de suponer que no para inscribirlos en el Obamacare[73].

Aunque la mayoría de los biopiratas piratean por una buena causa, no cabe duda de que entre la multitud habrá cierto número de manzanas podridas e incluso

elementos criminales. Con el tiempo, acabarán por existir equivalentes biológicos de todos los delitos informáticos graves actuales. Por ejemplo, piratear tu información genética podría muy bien ser el robo de identidad del mañana, sobre todo a medida que el ADN se utiliza de manera cada vez más extendida como método de autentificación. De hecho, la forma definitiva de robo de identidad es la clonación humana, y las barreras técnicas que la impiden están cayendo rápidamente, una eventualidad para la que la policía y la sociedad no están en absoluto preparadas. Así pues, no tenemos otra opción que considerar seriamente los pasos que es necesario dar para proteger el sistema operativo original del mundo.

La frontera final: espacio, nano y cuanto

> Hoy en día el mundo es muy diferente. Porque el hombre tiene en sus manos mortales el poder de abolir todas las formas de pobreza humana y todas las formas de vida humana.
>
> JOHN F. KENNEDY

Aunque el programa del transbordador espacial ya ha terminado, siguen realizándose muchas investigaciones y actividades en el campo de la ciencia espacial, sobre todo por parte de empresas privadas como SpaceX, de Elon Musk, o Virgin Galactic, de Richard Branson, que comercializan el transporte espacial. Otra de estas empresas, Planetary Resources, fundada en 2012 por Peter Diamandis y Eric Anderson, trata de poner al alcance de la humanidad los recursos naturales del espacio colocando robots sobre los asteroides para que los hagan explotar y conseguir así materias primas, mediante el uso de naves espaciales impresas en 3D a un coste bajísimo. Aunque resulte difícil de entender, tanto los delincuentes como los terroristas tratarán de emplear las tecnologías espaciales en su beneficio. Del mismo modo en que nadie previó el secuestro por parte de terroristas o la necesidad de policías aéreos cuando los hermanos Wright lograron aterrizar por primera vez con su avión en Kitty Hawk, también parece casi imposible considerar la necesidad de una policía espacial. Pero sin duda y por desgracia, ese día también llegará.

Por ahora, la mayor parte del interés de Crimen S. A. en el espacio se ha centrado en las tecnologías satelitales, y lo mismo puede aplicarse a las organizaciones terroristas. Como he señalado con anterioridad, Lashkar-e-Toiba utilizó tecnologías satelitales para las imágenes y las comunicaciones durante su brutal ataque a la población de Mumbai, y la insurgencia chií en Irak ha manipulado un *software* ruso barato pensado para robar la señal de las televisiones por satélite y lo ha usado para piratear la señal de vídeo de los VANT que rebota en los satélites estadounidenses confidenciales. En esa misma línea, unos piratas brasileños han utilizado antenas de

alto rendimiento y aparatos de fabricación casera para convertir los satélites de la Marina de Estados Unidos en sus propios comunicadores de banda ciudadana. Los satélites, a los que los piratas denominan *bolinhas* («bolitas»), han sido utilizados por todo el mundo, desde camioneros que circulan por la Amazonia y no tienen cobertura para sus móviles hasta organizaciones delictivas que envían mensajes codificados para alertar de las redadas policiales inminentes a los miembros de su banda y a los narcotraficantes en zonas remotas del país[74].

Tal vez un riesgo aún mayor para nuestro sistema global de satélites sería que agentes malintencionados trataran de destruir estos aparatos orbitales creados por el hombre alterando sus planes de vuelo y haciendo que choquen entre sí o con el creciente número de basura espacial[75]. En muchos aspectos, los satélites son un componente clave de nuestra infraestructura crítica de información global y son necesarios para servicios vitales como la previsión meteorológica, las comunicaciones de emergencia, los sistemas militares de alerta, la seguridad aérea y la navegación GPS. Existen precedentes de destrucción de satélites orbitales. En 2007, por ejemplo, China probó con éxito un arma antisatélite, que destruyó uno de sus propios satélites meteorológicos anticuados, algo que alarmó los gobiernos de Estados Unidos y de otros países[76].

El mismo efecto podría conseguirse fácilmente introduciendo *software* malicioso en el satélite o en su estación de control terrestre, o incluso lanzando un ataque de denegación de servicio contra un satélite. Tal ataque sería perfectamente posible según un boletín de la empresa de seguridad IOActive y el organismo gubernamental Computer Emergency Response Team[77]. De hecho, según desveló una comisión del Congreso, en 2007 las fuerzas armadas chinas interfirieron en el funcionamiento de dos satélites gubernamentales estadounidenses pirateando la estación terrestre que los controlaba desde Noruega[78]. Más recientemente, en 2014, se reveló que un grupo de piratas radicado en las oficinas del Ejército Popular de Liberación era el responsable de una serie de ataques en profundidad contra empresas satelitales tanto estadounidenses como europeas.

Los satélites no son lo único que se piratea: lo mismo sucede con las naves espaciales. Según un informe de 2008, un astronauta ruso llevó un ordenador portátil infectado a la Estación Espacial Internacional que difundió el virus W32.Gammima.AG por el sistema operativo informático de la EEI así como por varios ordenadores de a bordo con Windows XP[79]. En otro incidente de *malware* espacial, un astronauta infectó de manera accidental la EEI, esta vez con el virus Stuxnet, al conectar un dispositivo de memoria USB en la red informática de la estación[80]. Cargar un virus en la estación espacial mientras ésta sobrevuela nuestro planeta a trescientos cincuenta kilómetros de altura recuerda un poco a la escena de *Independence Day* en la que Will Smith y Jeff Goldblum transmiten un virus a la red espacial extraterrestre para salvar la Tierra, aunque al ser preguntado acerca del

malware que había infectado la EEI, un portavoz de la NASA contestó: «No ocurre a menudo, pero tampoco es la primera vez»[81].

Dentro de poco, delincuentes, terroristas y gobiernos canallas ya no tendrán que apropiarse de los satélites ajenos, pues serán capaces de lanzar los suyos propios. Nuevas tecnologías como la de los satélites en miniatura CubSats, tienen el tamaño de una caja de zapatos y no cuestan millones de dólares sino que pueden construirse y lanzarse por menos de cien mil. Estos aparatos podrán manejarse «fuera de la red», lo que significa que pueden lanzarse y controlarse fuera del alcance del gobierno, abriendo canales para comunicaciones por satélite privadas y encriptadas. El Chaos Computer Club de Berlín ya ha anunciado su intención de llevar Internet «más allá del alcance de los censores poniendo en órbita sus propios satélites de comunicaciones»[82]. Aunque está claro que la futura exploración espacial encierra un gran potencial para la humanidad así como algunos riesgos, aquí en la Tierra hay varias tecnologías emergentes que merecen un examen más detenido.

La nanotecnología es la manipulación de la materia a escala atómica y molecular, hasta llegar al nanómetro. Para entender lo pequeño que es un nanómetro, sólo hay que pensar que un pelo humano tiene ocho mil nanómetros de diámetro. Los científicos han puesto en marcha una revolución al tratar de crear máquinas de nivel molecular capaces de todo, desde reparar nuestros cuerpos hasta construir ordenadores ultrarrápidos. En 1991, las primeras fases de esta nanorrevolución produjeron una nueva forma de carbono con una nanoestructura cilíndrica conocida como nanotubo. Los nanotubos de carbono tienen propiedades materiales y eléctricas únicas que los convierten en herramientas extraordinariamente potentes para la miniaturización electrónica. El grafeno es otro poderoso nanomaterial descubierto en 2004 y que promete ser tan disruptivo como el plástico en su día. El «material milagroso» es cien veces más resistente que el acero, pesa seis veces menos y es mejor conductor de la electricidad que el cobre[83]. Puede que algún día se construyan puentes y aviones con ese material, y es probable que eso tenga un profundo impacto en el mundo de la electrónica. Según la Asociación Americana de Ingenieros Mecánicos, la nanotecnología «afectará prácticamente a todos los aspectos de la vida y se espera que en 2020 su uso se haya generalizado»[84].

Es posible que la mayor contribución de la nanotecnología tenga lugar en el campo de la medicina, en el que un nanobot terapéutico, mil veces más pequeño que una célula cancerígena, podría introducirse en el flujo sanguíneo con partículas de oro a nanoescala enlazadas con medicamentos contra el cáncer y dirigirse directamente al lugar exacto donde se halla el tumor[85]. Es más, la nanotecnología, igual que la biología sintética, puede ser una especie de materia programable, materia que puede cambiar sus propiedades físicas (como forma, densidad y conductividad) mediante un *input* de usuario o sensores automatizados. Estos materiales programables también pueden autoensamblarse como cadenas de ADN, mediante un enfoque de acumulación progresiva en el que las moléculas adoptan una disposición definida,

algo que la naturaleza hace de manera habitual pero que hasta el momento queda más allá del alcance de la ingeniería humana.

Aunque en la actualidad se limitan casi únicamente al campo de la investigación y el desarrollo, en el futuro las máquinas a nanoescala posibilitarán la creación de nanorrobots que acelerarán aún más los cambios exponenciales que tienen lugar en el ámbito de la robótica y la inteligencia artificial, creando algún día robots mil veces más pequeños que nuestras propias células. Estos *nanobots* tendrán enormes consecuencias en el campo de la robótica, pues podrán construir cualquier cosa, de cohetes espaciales a artefactos médicos inyectables. La nanotecnología tendrá también un impacto inmenso en el mundo del procesamiento informático, permitiendo construir ordenadores espectacularmente potentes: un nanoordenador del tamaño de un terrón de azúcar podría tener más capacidad de procesamiento de la que existe en el mundo actual[86].

Pero las cosas pequeñas pueden conllevar grandes peligros.

En su conocido libro de 1986 *Engines of Creation*, Eric Drexler argumentó que si las máquinas a nanoescala (ensambladores) pudieran construir materiales molécula a molécula, y luego utilizar miles de millones de estos ensambladores, sería posible construir cualquier material u objeto imaginable. Pero para alcanzar esa escala, los científicos tendrían que construir los primeros nanoensambladores en un laboratorio y darles instrucciones para que construyeran otros ensambladores, que a su vez construirían más, en un crecimiento exponencial con cada generación. No obstante, a Drexler le preocupaba que tal situación pudiera descontrolarse rápidamente cuando los ensambladores empezaran a transformar cualquier materia orgánica a su alcance en la siguiente generación de nanomáquinas, un proceso para el que acuñó la conocida expresión «escenario de plaga gris», en el que la Tierra podría verse reducida a una masa inerte invadida por nanomáquinas. ¿Cómo se llegaría a ese escenario apocalíptico? Supongamos que en el futuro se liberaran miles de millones de nanobots para limpiar un desastre ocasionado por un derrame de petróleo en el océano. Suena bien, si no fuera porque un pequeño error de programación podría llevar a los nanobots a consumir todos los objetos constituidos por carbono (peces, plantas, plancton, arrecifes de coral) en lugar de los hidrocarbonos del petróleo. Los nanobots podrían consumir todo lo que encontraran a su paso, «reduciendo el planeta a cenizas»[87]. Para entender la rapidez a la que tendría lugar este proceso, sólo hay que considerar el ejemplo que pone Drexler en su libro:

> Imagina un replicador flotando en un reservorio de elementos químicos, realizando copias de sí mismo […]. El primer replicador ensambla una copia suya en mil segundos, luego los dos replicadores ensamblan dos más en los siguientes mil segundos, esos cuatro construyen otros cuatro, y los ocho construyen otros ocho. Al cabo de diez horas, no hay 36 replicadores nuevos, sino más de 68 000 millones. En menos de un día, pesarían una tonelada; en menos de dos, sobrepasarían el peso de la Tierra; en otras cuatro horas, excederían la masa combinada del Sol y todos los planetas… si el reservorio de elementos químicos no se hubiera agotado mucho antes[88].

Aunque hay quien ha descartado la «plaga gris» por considerarla altamente improbable, otros, como se refleja en informes gubernamentales y de ONG, han considerado seriamente la posibilidad de que se plantee tal escenario y han dejado claro que hay clases de accidentes que la humanidad no puede permitirse[89]. Al cabo del tiempo, el propio Drexler aclaró sus comentarios y quitó importancia al escenario de la plaga gris considerándolo improbable[90]. Tenga o no lugar algún día una liberación accidental de nanobots autorreplicadores «biovoraces», el poder que entraña tal tecnología no pasará desapercibido a agentes maliciosos, incluidas organizaciones terroristas, que dentro de una década o más podrían explorar estas herramientas igual que hizo Aum Shinrikyo con su programa de armas químicas y biológicas en los años ochenta.

Otro campo científico emergente que encierra un gran potencial transformador para el ámbito de la informática es el de la física cuántica. Aunque queda mucho trabajo para conseguir que se generalice el uso de la computación cuántica y en muchas de las pruebas de sistemas ya existentes la realidad no ha coincidido con lo anunciado, los ordenadores cuánticos tienen el potencial para realizar cálculos a velocidades que dejarían por los suelos a los ordenadores actuales[91]. En una prueba llevada a cabo por Google y la NASA, un ordenador cuántico en desarrollo procesó varios algoritmos de prueba a una velocidad treinta y cinco mil veces mayor que la de los métodos de computación clásicos, utilizando servidores comerciales ya existentes[92]. Esto podría contribuir a resolver algunos de los problemas más difíciles del mundo, ya sea la búsqueda de nuevos tratamientos médicos o la creación de nanotecnología o inteligencia artificial de nueva generación[93].

Los ordenadores actuales son binarios, es decir, disponen tan sólo de dos valores posibles, el uno o el cero, conocidos como bits, para llevar a cabo el conjunto de sus instrucciones. Los ordenadores cuánticos, por su parte, se aprovechan de la idiosincrasia de las partículas subatómicas conocidas como cubits, que pueden ser un uno, un cero o una combinación simultánea de ambos[94]. En concreto, los ordenadores cuánticos tienen la capacidad de invalidar por completo todos los sistemas de seguridad informática que se usan habitualmente. En la actualidad, la seguridad informática se basa en la criptografía: utiliza la teoría de números y la multiplicación de números primos para codificar mensajes de manera que resulten ilegibles por parte de un tercero no autorizado. Para poder leer tus datos encriptados, hay que tener la clave matemática o bien se puede «atacarlos con fuerza bruta» realizando las operaciones necesarias una y otra vez para factorizar los números primos y que te proporcionen la solución correcta. Al introducir nuestras contraseñas, unos algoritmos encriptados las transforman en el factor correcto que abre el mensaje y proporciona la autentificación. Hoy en día, un ataque de fuerza bruta es algo a lo que la mayoría de los piratas informáticos no tiene que recurrir. En lugar de ello, confían en protocolos de encriptación mal implementados, *malware* informático, pulsaciones de teclado y errores humanos para robar la clave criptográfica necesaria

para leer los datos de tu tarjeta de crédito o tu información bancaria.

Sin la contraseña correcta, los piratas tendrían que aplicar la ingeniería inversa al proceso de encriptación, una gesta compleja y altamente improbable usando los ordenadores actuales. Incluso con un superordenador, un ataque de fuerza bruta tardaría miles de millones de años en desencriptar el cifrado AES de 128 bits que es el estándar en la actualidad (el universo tiene tan sólo 13 750 millones de años[95]). Mientras que los ordenadores clásicos sólo pueden realizar un único cálculo a la vez, los cuánticos pueden llevar a cabo un número enorme de cálculos aprovechando la naturaleza contraria a la lógica de la mecánica cuántica para alcanzar directamente la repuesta a preguntas muy complejas. En otras palabras, potencialmente, un ordenador cuántico podría atravesar los protocolos de cifrado, lo cual permitiría a su dueño leer el correo electrónico de cualquiera, hacer transferencias entre cuentas bancarias, controlar los mercados financieros, apropiarse de los sistemas de control del tráfico aéreo y manipular infraestructuras críticas. A la inversa, la tecnología cuántica también podría ser el avance que permita comunicaciones completamente seguras e inaccesibles, puesto que cualquier observación o interceptación de una clave de cifrado cuántico durante el tránsito cambiaría su contenido. Aunque no vas a poder adquirir uno de estos ordenadores en la Apple Store en un futuro cercano, numerosos gobiernos del mundo trabajan ya para construir ordenadores cuánticos capaces de *crackear* la criptografía actual y para desarrollar sus propias redes cuánticas seguras. No resulta sorprendente que la NSA haya gastado ya casi cien millones de dólares para crear un «ordenador cuántico criptológicamente útil» como parte de su proyecto Penetrating Hard Targets («Acceso a objetivos complejos»[96]). Hay que dejar claro que se trata de un problema tremendamente difícil de solucionar, pero la primera persona que lo haga concentrará un enorme poder en sus manos, algo que es probable que no mencione a todos aquéllos cuyas comunicaciones está leyendo y a cuyos sistemas accede.

Vistas en conjunto, las tecnologías más poderosas del siglo XXI, incluidas la robótica, la biología sintética, la fabricación molecular y la inteligencia artificial, tienen la capacidad de crear un mundo de una abundancia y prosperidad sin precedentes. Desde la creación ilimitada de energía hasta la producción de fuentes de recursos alimenticios inagotables, pasando por monumentales avances médicos, las tecnologías exponenciales pueden ser una extraordinaria fuente para hacer el bien.

Pero todos estos avances tienen también su reverso oscuro, como hemos visto una y otra vez en este libro. En el año 2000, Bill Joy, exjefe científico de Sun Microsystems, nos permitió vislumbrar hasta qué punto podían torcerse las cosas en un influyente artículo publicado en *Wired* titulado «Por qué el futuro no nos necesita»[97]. En él, Joy advertía claramente de que la robótica, la ingeniería genética y la IA amenazaban con convertir a los humanos en una «especie en peligro de extinción», puesto que las tecnologías exponenciales acabarían por superarnos y arrebatarnos el control. Joy señaló que nuestras tecnologías del siglo XXI se han

democratizado y que están disponibles para cualquiera con conexión a Internet. Hay clubes de robótica en los institutos y certámenes de biología sintética en las universidades. La IA copilota nuestros coches y es posible adquirir un VANT en Costco. Comparado con la amenaza nuclear, sin embargo, existe una incongruencia entre el poder potencialmente destructivo de estas tecnologías exponenciales y su actual disponibilidad para el ciudadano de a pie. Eso no quiere decir que deban prohibirse ni confinarse en laboratorios gubernamentales, dado el vasto potencial beneficioso que conllevarán, sobre todo en la medida en que se democratizan. ¿Quién sabe qué chico de Jaipur o qué abuela de Milwaukee, mientras se abren camino en el mundo de la biología sintética, realizará ese descubrimiento crucial en la lucha contra el cáncer que todos deseamos? Aunque es igual de probable que entre la multitud se escondan esos pocos sujetos malintencionados que pueden utilizar la misma tecnología para crear una pandemia global.

A pesar de que los ataques espaciales, la IA maliciosa y la plaga gris no se encuentren en los primeros puestos de nuestra lista de prioridades, encabezada por cosas como darse prisa para ir a recoger a los niños a la escuela, existe un gran número de amenazas que reclaman nuestra atención inmediata. Las infraestructuras críticas que hacen funcionar el mundo, desde nuestras redes eléctricas hasta los mercados financieros, están sometidas a ataques continuos, lo cual nos deja con una red de información global susceptible de sufrir un desplome sistémico inmediato. Al mismo tiempo, el volumen de datos que producimos sobre nosotros y las cosas que nos rodean crece de manera exponencial, lo cual plantea profundas cuestiones acerca de nuestra privacidad y las implicaciones éticas de lo que se convierte en posible gracias a los datos masivos y la incipiente sociedad de la vigilancia. Estos datos pueden ser pirateados y proyectados sobre un número siempre creciente de pantallas de nuestra vida para retratar «realidades» que de hecho son falacias. Esta falta de una ciencia informática que genere confianza se agrava aún más por la facilidad con la que pueden usarse algoritmos de caja negra para distorsionar nuestra realidad de forma apenas perceptible, algoritmos cuyos secretos sólo conocen aquellos que los programan a puerta cerrada y más allá del escrutinio de las masas.

La informática móvil y una Internet que crecerá metafóricamente del tamaño de una bola de golf al del Sol asoman por el horizonte, y pronto todos los objetos físicos estarán conectados a la red y se les asignará una dirección IP. Pero que haya más cosas en línea significa que hay más cosas que piratear, lo que permite a los sujetos malintencionados acceder a partes cada vez más íntimas de nuestra vida, de nuestro dormitorio a nuestro propio cuerpo, a medida que la biología se integra con las tecnologías de la información. Y en todo momento, delincuentes, terroristas y gobiernos canallas están ahí listos para explotar la inseguridad técnica común gracias a los numerosos fallos que persisten en los sistemas de *software* y de *hardware* actuales. Estos trabajadores del conocimiento ilegales del siglo XXI son profundamente innovadores y adaptativos, están en un proceso de aprendizaje

constante y se valen de las últimas prácticas empresariales, como la externalización o el *marketing* afiliado, para subvertir las tecnologías que nos rodean.

Los avances en informática e inteligencia artificial permiten que ahora los delitos se escriban, que funcionen de manera algorítmica, con un efecto mucho mayor, y que para ejecutarlos hagan falta muchísimos menos seres humanos. Pero las herramientas de que disponemos para detectar estas amenazas son desgraciadamente inadecuadas. El 95 por ciento de las amenazas de *malware* no se detectan y el tiempo para descubrir a un intruso en nuestras redes corporativas se aproxima a los 210 días: está claro que es posible penetrar cualquiera de nuestros sistemas y que aquéllos con tiempo y disposición para hacerlo, lo harán. De hecho, no es necesario mucho tiempo, como demostró el estudio del servicio secreto de Verizon: es posible introducirse en el 75 por ciento de todos los sistemas informáticos en cuestión de minutos, y sólo el 15 por ciento requiere unas cuantas horas para su pirateo.

El impacto de estas amenazas se notará aún más cuando el cibercrimen adopte el 3D, con miles de millones de objetos más conectados a la Internet de las Cosas, un mundo en línea emergente que también es sumamente pirateable y puede ser todavía menos seguro que nuestros ordenadores portátiles y teléfonos inteligentes. Los riesgos de la informática en tres dimensiones, encarnada por el auge de la robótica, significan que estamos creando máquinas con capacidad para superarnos y dominarnos, con un poder aún mayor gracias a su capacidad para actuar al unísono y trabajar como un enjambre para lograr sus objetivos. Este espectro representa una inquietante novedad dada la destreza física cada vez mayor de las crecientes legiones de robots militares armados, que se desplazan por aire, tierra y agua, la mayoría equipados con sistemas de inteligencia artificial para guiarlos y algunos dotados de autonomía letal para tomar por nosotros la decisión de matar. Así pues, la amenaza cibernética ha pasado de ser un problema puramente virtual a un peligro físico mundial. El resultado, como hemos visto a lo largo de este libro, es que la ciencia ficción se está convirtiendo en ciencia a secas delante de nuestros ojos.

Con la aparición de Internet y la inminente llegada de los miles de millones de conexiones adicionales que permitirá la Internet de las Cosas y sus sensores, nuestro planeta ha desarrollado un sistema nervioso en continua expansión. Éste conecta nuestras comunicaciones, nuestros pensamientos e incluso nuestros cuerpos con un cerebro en línea global de una complejidad tremenda, controlado por una plétora de sistemas de *software* y protocolos de red de los que se puede aprovechar en cualquier momento cualquiera que quiera hacernos daño. Lamentablemente, el sistema inmunitario que protege este sistema nervioso global es débil y sufre ataques constantes. No hay que subestimar las consecuencias del fallo del sistema. Por ello, es hora de empezar a diseñar, proyectar y construir sistemas de autoprotección mucho más robustos, salvavidas que puedan crecer y adaptarse a la misma velocidad a la que surgen las nuevas amenazas tecnológicas en nuestro mundo. Aunque resulta fácil centrarse sólo en los abundantes beneficios que la tecnología aporta a nuestras vidas,

si ignoramos los peligros que la acompañan, será por nuestra propia cuenta y riesgo.

Estamos viviendo en una era exponencial y sin embargo, psicológicamente, nuestro cerebro sigue siendo el mismo que el de los cazadores de la Edad de Piedra: apenas se ha actualizado a lo largo de los últimos cincuenta mil años. Así pues, no forma parte de nuestra naturaleza entender el poder inherente de las tecnologías exponenciales. Pero debemos intentarlo. Porque, igual que las criaturas que viven en el proverbial estanque cubierto de nenúfares mencionado previamente, estamos sujetos a amenazas debidas al cambio exponencial. Para los estudiantes franceses a los que se advirtió de que disponían de treinta días para actuar con el objetivo de salvar el estanque, en el día 25 apenas había nada de lo que preocuparse porque el nenúfar sólo cubría el 3 por ciento del estanque, así que lo dejaron crecer. Como ya sabemos, al llegar al día 29 el nenúfar había crecido milagrosamente hasta cubrir la mitad de la superficie del agua, pero para entonces quedaba ya muy poco tiempo para salvar el estanque, que al día siguiente fue engullido por el nenúfar. En la actualidad puede resultar sencillo ignorar la totalidad de nuestra inseguridad tecnológica. Sí, por supuesto, de repente piratean unos millones de cuentas por aquí y roban mil millones de contraseñas por allí, pero nos queda tiempo. Drones, marcapasos, control aéreo, coches, farolas, sistemas de navegación, máquinas de IRM: todo pirateado. Pero nos queda tiempo. Decenas de miles de millones de objetos nuevos que se añadirán a Internet, pero nos queda tiempo. ¿O no?

La suerte está echada. La tecnología hace que estemos cada vez más conectados, que seamos más dependientes y vulnerables. Aunque los innumerables avances que posibilita la tecnología exponencial auguran grandes y desconocidos beneficios para la humanidad, es necesario guiarlos y protegerlos de aquellos que los aprovecharían para hacer daño a los demás. Si ignoramos las abrumadoras pruebas del peligro tecnológico que nos rodea, será por nuestra cuenta y riesgo. El día 29 se acerca con rapidez. ¿Qué vamos a hacer al respecto?

Tercera Parte

Sobrevivir al progreso

Capítulo 17

Sobrevivir al progreso

> Para mí es mucho mejor captar el universo como es en realidad que persistir en el engaño, por muy satisfactorio y reconfortante que sea.
>
> CARL SAGAN

Ha sido un viaje duro. Se nos ha pedido que nos planteemos interrogantes difíciles y a menudo incómodos acerca de la tecnología y el papel de las máquinas omnipresentes en nuestras vidas, dispositivos a los que hemos dado la bienvenida en nuestros hogares, oficinas, ciudades e incluso en nuestros cuerpos sin demasiada reflexión al respecto. Y ahora el viaje nos ha conducido a observar con ojos más penetrantes y críticos el número creciente de pantallas informáticas que proliferan en nuestro mundo, pantallas a las que hemos dado una vuelta de 180 grados para mostrar el otro lado de la historia, el peligro, además de la promesa, que entraña nuestro idilio con la tecnología. La interconexión cada vez más extendida y la ubicuidad de sistemas informáticos inherentemente vulnerables implican que la tormenta de seguridad tecnológica que se está formando en el horizonte no puede seguir pasándose por alto.

El problema, por supuesto, no es que la tecnología sea algo malo, sino que tan pocos la entiendan. Como consecuencia, quienes sí tienen conocimientos en la materia pueden subvertir el código informático que hace funcionar nuestro planeta y utilizarlo en nuestra contra. Los tiempos exponenciales están llevando a delitos exponenciales, delitos en los que individuos malintencionados que actúan en solitario podrán afectar negativamente a millones de personas en cualquier lugar y en cualquier momento. En efecto, toda la gama de infraestructuras de información esenciales que sirven de motor a nuestra sociedad están en riesgo. Estos desafíos se verán enormemente exacerbados a medida que miles de millones de objetos nuevos se conecten a Internet y ordenadores en red en forma de robots empiecen a desplazarse por el espacio físico que compartirán con nosotros, por no mencionar los riesgos que entrañan la inteligencia artificial y la biología sintética. El panorama pinta desalentador y abrumador, pero sólo si primero entendemos e identificamos estas amenazas podremos empezar a efectuar los cambios necesarios para apuntalar los cimientos futuros del mañana tecnológico.

No existe una manera fácil de enmendar la situación en la que actualmente estamos inmersos. No existe una panacea ni una solución sencilla al estilo de «añada agua y agite bien» que vaya a solucionar nada. Miles de millones de pequeños pasos

nos han conducido a este dilema y tendremos que dar otros miles de millones de pasos más para salir del aprieto. La naturaleza asimétrica de la amenaza implica que a los atacantes les basta con detectar una única debilidad, mientras que los defensores deben proteger de todas ellas, un verdadero imposible. Dicho esto, no está todo perdido ni hay que abandonar toda esperanza. Ni necesitamos ni nunca conseguiremos una «seguridad perfecta». Sencillamente porque no existe. Ahora bien, la ausencia prácticamente absoluta de una computación fiable en un mundo regulado por los ordenadores debería servirnos de señal de advertencia a todos.

No cabe duda de que la ciencia y la tecnología han sido un activo neto positivo para la humanidad. No obstante, para prosperar en el siglo que viene, primero debemos sobrevivir a los riesgos tecnológicos que inevitablemente conlleva este progreso. Es fundamental adoptar medidas hoy, cambiar de rumbo, para desviarnos del futuro peligroso que se avecina. Las páginas siguientes recogen una serie de recomendaciones técnicas, organizativas, educativas y de políticas públicas, tanto estratégicas como tácticas, destinadas a reducir los riesgos que entraña la tecnología y que actualmente se multiplican de manera exponencial. De la infinidad de pasos que debemos dar para proteger nuestro futuro tecnológico, considero que los siguientes son los más importantes. La tecnología forma parte de nuestras vidas y no hay vuelta atrás. La cuestión principal es cómo utilizar estas herramientas para lograr el máximo bien posible a la par que se minimizan los inconvenientes. He aquí cómo podríamos sobrevivir al progreso.

Aplicaciones asesinas: *software* dañino y sus consecuencias

> Cada vez que reciben una actualización de seguridad […] lo que sea que se ha actualizado es porque se ha transgredido y ha quedado expuesto, vulnerable, durante quién sabe cuánto tiempo. A veces son días y a veces años.
>
> QUINN NORTON

Los programadores del *software* de Facebook se han guiado siempre por el mantra «Move fast and break *things*» («Muévete rápido y rompe cosas»). Este lema, que se estampó en letras grandes en las paredes de la sede de la empresa, reflejaba el comportamiento propio de piratas informáticos de Facebook, según el cual, aunque las nuevas funciones o herramientas de *software* no fueran perfectas, la velocidad era la clave en la creación de código, por mucho que pudiera provocar problemas o fallos de seguridad. Según declaraciones del propio Zuckerberg: «Si nunca rompes nada, probablemente es que no te mueves lo bastante rápido»[1]. Facebook no es el único que aplica estas prácticas de codificación de *software*. Ya sea a las claras o a las

oscuras, gran parte del sector del *software* se rige por una variante del lema «Envíalo y ya está» o «La perfección está sobrevalorada». Muchos programadores envían de manera consciente *software* que admiten que es «una birria», pero ahí lo dejan, con la esperanza, quizá, de hacerlo mejor la próxima vez. Estas actitudes son emblemáticas de todos los errores de la programación de *software* y representan quizá la mayor amenaza contra la seguridad informática en el presente.

El público en general quedaría conmocionado si supiera que la mayor parte de la tecnología que nos rodea funciona a duras penas y está montada apresuradamente mediante la llamada *duct-tape programming* («programación con cinta adhesiva»), siempre a unas pocas pulsaciones de que el sistema se cuelgue. Tal como Quinn Norton, un periodista de la revista *Wired* encargado de cubrir a la comunidad de piratas informáticos, ha señalado: «El *software* es una basura»[2]. La mayoría de los programadores informáticos están sobrepasados de trabajo, cobran poco y les imponen plazos de entrega apretados. Lo único que les apetece es regresar a sus casas para estar con sus hijos y, como consecuencia, lo que circula es un *software* defectuoso, incompleto, repleto de agujeros en la seguridad, causante de incidentes como Heartbleed o de ataques de piratería a gran escala como los acometidos contra Target, Sony y Home Depot.

Programar hoy en día no es una tarea fácil; muy al contrario, es increíblemente compleja. Con cerca de cincuenta millones de líneas de código individuales en Microsoft Office y la necesidad de que cada una de ellas funcione a la perfección para mantener a raya a los atacantes, no es de extrañar que algo se tuerza. Y estamos hablando de un solo programa. Tu ordenador o *smartphone* tiene armonizar y supervisar todos los programas que utiliza, por no mencionar ya los que se ejecutan en otros sistemas con los que desea interactuar en cada una de las páginas web que visitas. Este problema se multiplica exponencialmente a medida que más y más dispositivos de la Internet de las Cosas empiezan a comunicarse entre sí. Todos esos errores de *software* (*bugs*) y fallos de seguridad tienen un efecto acumulativo en la red de información mundial, lo cual explica que el 75 por ciento de nuestros sistemas puedan vulnerarse en cuestión de minutos. Tal complejidad, combinada con una honda actitud relajada por lo que respecta a los errores de *software*, ha llevado a Dan Kaminsky, un respetado investigador en materia de seguridad informática, a observar que hoy en día «gracias al Código, vivimos inmersos en la Era de la Cólera»[3].

Cuando se los increpa por el lamentable estado del *software* que circula por el mundo en la actualidad, muchos programadores replican: «Somos humanos. El *software* perfecto no existe». Y tienen razón. Pero estamos muy lejos de «rozar la perfección», quizá al 50 por ciento de donde podríamos y deberíamos estar, de acuerdo con Charlie Miller, un reputado investigador de temas de seguridad[4]. El mero hecho de ampliar esa cifra a un 70 o un 80 por ciento podría suponer una inmensa diferencia para la seguridad de la informática en general. Los consumidores demandan *software* lleno de funciones y potente, y lo quieren ya; decenas de miles de

personas están dispuestas a hacer cola durante días, durmiendo en las aceras, para conseguir el último modelo de iPhone. Pero es imperativo que los fabricantes apuesten mucho más fuerte y coloquen el diseño de seguridad entre sus máximas prioridades, de tal manera que se convierta en un elemento clave de una computación fiable.

Para cambiar el rumbo de este barco, deberán alinearse incentivos con el fin de garantizar que el énfasis tan necesario en la informática segura acabe por convertirse en una realidad. Por ejemplo, actualmente, cuando los *hackers* detectan una vulnerabilidad en un programa de *software*, pueden vendérsela en el mercado negro a Crimen, S. A. por un precio considerable o bien comunicársela al fabricante por una propina a la par que afrontan una amenaza de juicio. Y, como es lógico, se decantan por la opción evidente. A pesar de que esta situación está empezando a cambiar y algunas empresas han establecido «programas de recompensas por *bugs*», pocas ofrecen recompensas económicas y las pocas que sí lo hacen entregan cantidades muy inferiores a las que se barajan en la clandestinidad digital. Eso tiene que cambiar. Crear sistemas de comunicación de vulnerabilidades a la seguridad bien remunerados que paguen a los *hackers* por poner en conocimiento de los fabricantes los fallos importantes ayudaría a minimizar los daños que estas empresas informáticas generan cuando lanzan de cualquier manera y apresuradamente código defectuoso e inseguro a un público confiado.

Además, habida cuenta que el *software* es el motor que mueve la economía mundial y todas nuestras infraestructuras críticas, desde el tendido eléctrico hasta el sistema telefónico, no hay tiempo que perder. Ahora bien, no basta con que unos cuantos investigadores en materia de seguridad escriban artículos convincentes sobre este tema; es preciso escuchar el clamor del público, un clamor inexistente hasta el presente que exija un *software* de mejor calidad. Reflexiona sobre ello unos instantes. ¿Por qué aceptamos todos estos errores y fallos como si fueran algo natural? No tienen por qué serlo. Y podemos hacer que dejen de serlo si exigimos responsabilidades por sus acciones a las empresas del sector del *software*, que mueve 150 000 millones de dólares al año[5]. En ausencia de esta exigencia por parte del público, en la batalla entre la rentabilidad y la seguridad, siempre saldrán ganando los beneficios. Debemos hacer que las empresas entiendan que el programar código más seguro forma parte de sus intereses a largo plazo y que lo contrario acarreará consecuencias. Hoy por hoy, los ingenieros, programadores y las empresas que crean las tecnologías del presente no tienen prácticamente ninguna responsabilidad ni personal ni profesional por las consecuencias de sus acciones. Ha llegado el momento de que eso cambie.

Daños provocados por el *software*

El destacado profesor de ciencia informática de Yale Edward Tufte observó en su día que sólo hay dos sectores que se refieren a sus clientes como usuarios: los programadores informáticos y los traficantes de drogas. Y lo que es más importante, es igual de improbable que te recuperes de los daños que provocan sus productos[6]. El fondo de la cuestión es que, cuando aceptas con un clic los extensos términos y condiciones de servicio sin leértelos, accedes a utilizar el *software* de la empresa o servicio de Internet «tal cual» y, por ende, toda responsabilidad por los posibles daños recae en ti. Estas empresas utilizan expresiones como «nos eximes, tanto a nosotros como a nuestros afiliados, agentes, oficiales y empleados, de cualquier reclamación, demanda o acción derivada o relacionada con el uso de estos Servicios» o «no garantizamos que nuestro producto siempre sea seguro ni carezca de errores». ¿Te comerías un burrito mexicano con chipotle si te lo suministraran con una advertencia así? Intuyo que no. Entonces ¿cómo se las ha apañado la industria del *software* para eximirse de toda responsabilidad? Buena pregunta.

Cuando un automóvil tiene un accidente debido a un fallo en las conexiones o a un *firmware* erróneo, como hemos visto que pasó en los casos de aceleración mortal de Toyota, los afectados pueden interponer una demanda por daños. Entonces, ¿por qué no se puede hacer lo mismo con el *software*? ¿Es razonable sugerir que si alguien muriera o sufriera graves pérdidas económicas como resultados de un *software* defectuoso se les negaría la posibilidad de acudir a los tribunales porque los términos de servicio así lo recogen? ¿Incluso aunque pudiera demostrarse ante un juez y un jurado que el *software* fue la causa inmediata del daño? A mí no me lo parece.

No me malinterpretes. No es que sea aficionado a crear nuevas leyes guste o no guste. Y tampoco apuntaría que la legislación es la mejor manera de abordar la totalidad de la ciberinseguridad mundial que padecemos. En el mejor de los supuestos, es un arma roma en un campo que evoluciona a pasos tan agigantados como la tecnología. No obstante, es preciso dibujar una línea en la arena. Hacer caso omiso de manera temeraria a todas las consecuencias del *software* mal programado, lanzado al mercado con vulnerabilidades conocidas y endilgado a un público incapaz de leer por sí solo los millones de líneas de código de sus teléfonos móviles y ordenadores portátiles para sopesar los daños concomitantes sencillamente no es correcto. Quienes programan y crean estas herramientas deben asumir cierta responsabilidad.

Huelga decir que la industria del *software* se opone tajantemente a este tipo de cambios. Afirma que permitir demandas por responsabilidad tendría unas repercusiones catastróficas en su rentabilidad y la conduciría a la bancarrota. Y también argumenta que la complejidad de las interacciones del *software* es tal que sería imposible adjudicar de manera justa las culpas en caso de llegarse a juicio. Ambos argumentos son insatisfactorios. Ya los vimos en el pasado, en concreto en el sector automovilístico, cuyos productos a lo largo de la década de 1960 presentaban unos niveles de seguridad nefastos. Gracias a las demandas de los consumidores y a

las actuaciones de algunos congresistas, en 1966 se aprobó finalmente la Ley de Seguridad del Tráfico Nacional y los Vehículos Motorizados en Estados Unidos, que permitió al gobierno imponer normativas de seguridad a la industria automovilística. Y hacerlo redundó en uno de los mayores logros en temas de salud pública del siglo XX. Las muertes por accidente de tráfico descendieron estrepitosamente y se salvaron decenas de miles de vidas[7].

Es innegable que la tecnología actual es más compleja que los automóviles del pasado, pero no conseguiremos ninguna mejora en la seguridad de sus productos de *software* y *hardware* hasta que los incentivos empresariales se alineen con la exigencia de un cambio. Hoy por hoy, cualquier daño que sufran los usuarios finales es cosa suya y sólo suya, y prácticamente no puede achacarse nada a la responsabilidad de los fabricantes del *software*. Y puesto que las consecuencias por lanzar al mercado código defectuoso son prácticamente nulas, esta práctica prosigue su camino. A menos que los responsables de los problemas de seguridad subyacentes que crean deban asumir sus acciones, no cambiará nada. Sólo cuando los costes empresariales de poner en circulación código que se vulnera de manera persistente sean mayores que solucionar las vulnerabilidades conocidas por anticipado, la balanza se inclinará en favor de un código mejor y más seguro. Y pese a que no abogo por la creación de nuevas regulaciones de amplio alcance ni burocracias gubernamentales, creo firmemente que cabe iniciar un debate público vigoroso en torno a las causas subyacentes de la inseguridad informática generalizada. Ha llegado el momento de poner en orden nuestra casa de programación y *software*, antes de que añadamos los próximos cincuenta mil millones de cosas a la red de información mundial.

Reducir la contaminación de datos y exigir privacidad

A todo lo largo de este libro hemos analizado las consecuencias de amasar petabytes y petabytes de datos, información que con el tiempo acaba filtrándose. Ya se trate de informes médicos personales, balances bancarios, secretos gubernamentales o propiedad intelectual empresarial, todo se filtra. El almacenamiento masivo de estos datos en manos de unas cuantas empresas de datos y los gigantes de Internet genera unas dianas irresistibles de atacar, una suerte de tiendas donde los delincuentes pueden encontrar de todo. Tal como he dicho antes, cuantos más datos se producen, más deseosa de consumirlos se muestra la delincuencia organizada.

Pese a que la mayoría de los internautas han elegido compartir de manera voluntaria algunos de los detalles más personales de sus vidas a través de las redes sociales en línea, las empresas situadas tras esos servicios recopilan muchos más datos de los que la mayoría somos conscientes. Quienes suministran servicios de

Internet «gratuitos» rastrean de manera constante a los usuarios durante toda su experiencia online, así como sus movimientos en el mundo físico mediante el uso que hacen de sus teléfonos móviles. Sin embargo, tal como hemos visto, las cosas más caras en la vida son gratis. Toda esta información se segmenta, cuartea y vende al mundo tenebroso y oculto de los agentes intermediarios de datos, quienes ejercen un control escaso o nulo sobre la precisión o la seguridad de la información que retienen. Y si bien podríamos quejarnos por tales prácticas (si fuéramos los verdaderos clientes de estas empresas de redes sociales), no tenemos derecho a hacerlo. Hemos cedido esos derechos a cambio de una cuenta de correo electrónico gratuita, actualizaciones de estado y fotografías en línea, cesión que hemos aceptado al hacer clic en un contrato de términos y condiciones de servicio de cincuenta páginas de extensión y con un cuerpo de letra de cuatro puntos que absolutamente nadie se lee. Estos «contratos» unilaterales y a todas luces extralimitados no deberían absolver a las empresas que los escriben de todas las responsabilidades relativas a cómo conservan y guardan nuestros datos. Si deciden conservar cada migaja de pan sobre nuestras vidas, entonces deberían ser responsables de las consecuencias.

Lo más alarmante acerca de este sistema es que no había motivo para organizarlo así. Se calcula que cada usuario de Facebook del mundo sólo genera unos ocho dólares anuales en ingresos por publicidad (no beneficios) a la empresa[8]. Personalmente, yo preferiría enviarle diez dólares a Facebook y que me dejaran en paz. Por menos de un dólar al mes, es unas cien veces más barato que mi factura de televisión por cable. Es un sistema insano. Tal como ha proclamado el investigador del MIT Ethan Zuckerman, «La publicidad es el pecado original de la Red. Toda la deshonra de Internet es una consecuencia directa, pese a no ser intencionada, de elegir la publicidad como el modelo por defecto para financiar el contenido y los servicios en línea»[9]. Pese a que nuestros datos pagan por Gmail, YouTube y Facebook en la actualidad, también podríamos dar nuestro apoyo a aquellas empresas de Internet cuyo objetivo fuera almacenar el mímino de datos personales acerca de nosotros a cambio de sumas mínimas de dinero. ¿Por qué no eliminar al intermediario en pro de un sistema mucho más lógico? Pasaríamos a ser los clientes de Facebook y de Google por un dólar al mes y podríamos seguir disfrutando de la vida.

Por desgracia hoy, como en el caso de los fabricantes de *software*, los incentivos no están bien alineados desde la perspectiva de la seguridad pública. El incentivo de Facebook es recabar una cantidad incesante de datos identificables personalmente acerca de sus clientes para venderlos a miles de agentes intermediarios de datos de todo el mundo y obtener beneficios. Tal es su modelo de negocio. Y si los compradores finales de esta información acaban permitiendo que se utilice para cometer usurpación de identidad, acoso o espionaje industrial poco importa a las empresas de redes sociales una vez han subastado la información al mejor postor. Pero sí que nos importa a nosotros, que somos quienes sufrimos los perjuicios económicos y sociales resultantes de la filtración de datos. Y si hay quien prefiere los

beneficios del sistema «gratuito», pues que lo disfrute con todo lo que comporta. Pero ¿por qué no ofrecernos al resto la opción de pagar por mantener un mayor control de nuestra privacidad y seguridad?

Si bien sería imposible «vivir sin la Red» en el mundo moderno, sería perfectamente posible diseñar un sistema mucho más protector. Ya existen ejemplos mejores y más equilibrados, como la Directiva de Protección de Datos de la UE, que tiene mucho más en cuenta al consumidor y consagra la privacidad como un derecho fundamental de todos los ciudadanos europeos. Limita qué datos y durante cuánto tiempo pueden almacenar las empresas antes de tener que eliminarlos. Se trata de un planteamiento más sensato que no sólo equilibra la inclinada balanza del poder en nuestra relación con las empresas de Internet, sino que además nos protege y evita que nuestros datos se filtren y vayan a parar a manos de Crimen, S. A.

Acabar con las contraseñas

Tal como vimos en el primer capítulo, cuando analizamos el caso del ataque de piratería épico dirigido contra Mat Honan, una secuencia de caracteres alfanuméricos ya no puede protegernos. Desde luego, puedes darte un mayor margen de tiempo configurando una contraseña de veinticinco dígitos que alterne letras en mayúsculas y minúsculas, números y símbolos, pero lo cierto es que nadie lo hace. En su lugar, incluso en 2015 las contraseñas más populares siguen siendo «123456» y «password». El 55 por ciento de las personas utilizan la misma contraseña en la mayoría de los sitios web y el 40 por ciento ni siquiera protege sus teléfonos inteligentes con contraseña[10]. Y aunque lo hicieran, no les serviría de mucho. Dados los avances en el poder computacional, el procesamiento en la nube y el *crimeware* registrados en la clandestinidad digital, más del 90 por ciento de las contraseñas pueden descifrarse en cuestión de pocas horas, según un estudio de Deloitte Consulting[11]. Aún peor, las empresas de Crimen, S. A., como la rusa CyberVor, han recopilado más de 1200 millones de nombres de usuario y contraseñas con los cuales pueden desbloquear cuentas a su antojo. En pocas palabras: nuestro sistema actual de usar un nombre de usuario y una contraseña no sirve de nada.

Es posible adoptar algunas medidas que nos proporcionarán capas adicionales de protección. Un ejemplo de éstas es la autenticación de doble factor que ofrecen Google, Microsoft, PayPal, Apple y Twitter, entre otros, la cual combina tu nombre de usuario y contraseña con identificador de seguridad, un llavero de clave dinámica o un teléfono móvil. La mayoría de las empresas de Internet para consumidores recurren a tu teléfono móvil como segundo factor enviándote un código único mediante un mensaje de texto que debes introducir para poder acceder a tu cuenta. De este modo, incluso aunque un pirata informático lograra colarse en tu cuenta

bancaria, servicio de red social o perfil de red social, necesitaría acceder además a tu teléfono y mensaje de texto, cosa que muy probablemente no podría hacer si tú y tu teléfono estáis en Nueva York y él está en Moscú. Si bien la autenticación de doble factor es sin duda un paso en la dirección correcta, estos sistemas también pueden vulnerarse mediante ataques con intermediario, que interceptan los mensajes de texto mediante *software* malicioso para teléfonos móviles.

A tal fin, muchas empresas de *smartphones*, como Apple y Samsung, avanzan hacia otra forma de seguridad de doble factor, consistente en combinar algo que sabes con algo que eres, como tu huella biométrica o la identidad de tu voz. Tu huella dactilar irá reemplazando progresivamente a tu contraseña y con la salida al mercado del iPhone 6 y el iOS 8, Apple ha permitido a otras empresas, como PayPal y algunas entidades bancarias, utilizar el sensor de huella dactilar Touch ID de tu teléfono para autenticarte. Y pese a que los piratas informáticos, como el Chaos Computer Club, y otros agentes han subvertido algunos de estos sistemas en el pasado (si tenían acceso al dispositivo), la autenticación multifactor puede proporcionar una mejora significativa con respecto al nombre de usuario con contraseña estándar. Mat Honan tenía razón. Es hora de olvidarnos de las contraseñas y avanzar hacia una autenticación multifactor y la biométrica, herramientas que, pese a distar mucho de ser perfectas, constituyen una mejora inmensa frente a los débiles caracteres alfanuméricos que utilizamos en la actualidad. Pese a que en la actualidad no existe una panacea para la identificación del usuario, sí existen oportunidades tremendas de plantear alternativas sensiblemente mejores, sobre todo mediante esfuerzos de investigación y financiación coordinados, como analizaremos en breve.

Encriptación por omisión

> Sólo existen dos clases de empresas: las que han sido pirateadas y las que lo serán.
>
> ROBERT MUELLER, exdirector del FBI

La inmensa mayoría de los datos actuales no están encriptados o cuentan con una protección muy pobre. Un estudio acometido por el gigante de la informática HP en julio de 2014 reveló que el 90 por ciento de los dispositivos que tenemos conectados recopilan datos personales, el 70 por ciento de los cuales se comparten en red sin ningún tipo de encriptación[12]. Eso implica que cualquiera que obtenga acceso a un sistema informático con *software* programado de manera deficiente, donde se haya descargado *software* malicioso o en el que se hayan usado contraseñas débiles, puede robar, leer y utilizar cualquiera de los datos contenidos en el sistema. Sin encriptación, cualquiera que acceda a los datos puede leerlos. Eso explica que

Crimen, S. A. pueda utilizar los cincuenta y cinco millones de tarjetas de crédito robadas a Home Depot, porque el sistema de pagos de los comercios de la empresa no encriptaba los datos de crédito de los clientes que tenía en memoria[13]. De haber estado debidamente encriptados esos datos, habrían carecido de valor para los ladrones que los robaron. Ahora bien, no sólo los datos financieros suelen almacenarse sin encriptar, sino también historiales médicos, secretos empresariales, retransmisiones de vídeo enviadas por drones militares, fotografías de famosos desnudos y prácticamente todo el correo electrónico. La repercusión de las infiltraciones informáticas y el robo de datos podría minimizarse sobremanera si la aplicación de una encriptación debida se convirtiera en la práctica estándar por omisión.

La mayoría de los datos almacenados tanto en discos duros personales como empresariales se guardan en texto simple, legible por cualquiera que tenga acceso a estos dispositivos. Y lo mismo ocurre con una parte leonina del tráfico que se entrecruza en Internet, salvo el de los grandes sitios web que utilizan HTTPS al enviarte información sobre tu contraseña o tarjeta de crédito. Ahora bien, podemos mejorar sustancialmente en este aspecto, sobre todo en la estela de las revelaciones de Edward Snowden. Por la cara positiva, Google encripta cada vez más su tráfico entre tu ordenador y sus servidores (no sólo tu contraseña), incluidos todos los mensajes de Gmail. Hacerlo dificulta enormemente que otra persona pueda interceptar y leer tus mensajes de correo electrónico en tránsito; de otro modo, cualquier mensaje que envíes es como si estuviera escrito en una postal y pudiera acceder a él cualquiera que lo vea a su paso por Internet, por ejemplo si te conectas por Wi-Fi en la cafetería Starbucks de tu barrio. La Electronic Frontier Foundation, una fundación sin ánimo de lucro que aboga por los derechos digitales y la privacidad, también ha lanzado un programa conocido como «HTTPS Everywhere» («HTTPS ubicuo») para fomentar el uso de la encriptación en todo el tráfico de los navegadores de Internet. En suma, es hora de encriptar Internet para proteger la privacidad y la seguridad de nuestras comunicaciones digitales y datos informáticos.

Si bien los sistemas operativos informáticos actuales, incluidos los de Microsoft y Apple, se entregan con herramientas de encriptación del disco duro gratuitas incorporadas, no vienen activadas por omisión y sólo una reducida minoría de las empresas y un mínimo porcentaje de consumidores encriptan los datos de sus ordenadores portátiles y de sobremesa. De hecho, la mayoría de los consumidores ni siquiera saben que estos protocolos de seguridad existen. En la estela del gran *fiasco* de la piratería contra el iCloud de celebridades, el director ejecutivo de Apple, Tim Cook, reconoció que la empresa debía esforzarse por incrementar la conciencia de sus clientes en temas de ciberseguridad. Estoy completamente de acuerdo. En septiembre de 2014, Apple anunció que su último iPhone encriptaría todos los datos en el dispositivo cuando se configurara una contraseña, un movimiento que Google se comprometió a incorporar también a su próximo sistema operativo para teléfonos

móviles Android. Son pasos importantes para minimizar los riesgos de seguridad de los teléfonos inteligentes, pero, dado que el 40 por ciento de los usuarios ni siquiera utilizan contraseña en sus móviles, Tim Cook tenía razón: hay que fomentar la educación y la conciencia entre el público.

La educación, el arma contra la ciberdelincuencia

La civilización vive una carrera entre la educación y la catástrofe.

H. G. WELLS

En Estados Unidos y en todo el mundo hay un problema de analfabetismo, y no es el que la mayoría de nosotros tenemos en mente. Me refiero al analfabetismo técnico. En un mundo repleto de artilugios, algoritmos, ordenadores, tecnología ponible, chips de identificación por radiofrecuencia y teléfonos inteligentes, sólo una parte ínfima de la población en general tiene alguna idea de cómo funcionan estos objetos. Y ya sea Crimen, S. A. o la NSA, quienes saben programar poseen el poder sobre quienes no saben, del mismo modo que quienes no sabían leer y escribir en el siglo pasado tenían menos posibilidades de prosperar en la vida. Tenemos que proporcionar conocimientos técnicos al público en general.

El objetivo no es que todos nos volvamos programadores informáticos (pese a que fomentar los conocimientos en ciencia, tecnología, ingeniería y matemáticas del país iría de fábula a nuestra economía). El objetivo es que los ciudadanos comprendan al menos en un nivel básico cómo funcionan las tecnologías que los rodean, no sólo para que puedan sacar el máximo partido de estas herramientas, sino también para que otras personas no puedan aprovecharse de su ignorancia tecnológica y hacerles daño. Si a Cassidy Wolf, Miss Teen USA, le hubieran enseñado en la escuela el simple truco de tapar la *webcam* con una notita *Post-it* amarilla, ningún pirata informático habría podido tomar en secreto fotografías de ella desnuda en su propio dormitorio. Por supuesto, es sólo un ejemplo, pero, caso tras caso de ciberataque, si la víctima hubiera estado armada con el conocimiento adecuado de cómo protegerse, el dolor del ataque podría haberse evitado por completo. La educación es clave y nuestra educación en materia de ciberseguridad es pésima.

En las escuelas públicas de Estados Unidos proporcionamos a los niños todo tipo de formación, desde vial hasta sexual. Sin embargo, es probable que tus hijos pasen mucho más tiempo navegando por Internet e interactuando con tecnologías que manteniendo relaciones sexuales o conduciendo. Y pese a ello, la mayoría de las escuelas ofrecen una educación mínima o nula acerca de cómo utilizar la Red de manera segura. Durante años, la serie de dibujos animados *McGruff, el perro del*

delito, creada por el Consejo Nacional para la Prevención de la Delincuencia de Estados Unidos, fue un elemento fijo en los televisores y las escuelas estadounidenses con el fin de prevenir la delincuencia tanto en niños como en adultos. Hoy más que nunca necesitamos que el sabueso McGruff enseñe a nuestros niños a mantenerse alejados de la ciberdelincuencia. Por suerte, ya están en marcha algunos programas de gran utilidad. El Consejo Nacional para la Prevención de la Delincuencia en Estados Unidos ha lanzado programas para informar a padres e hijos acerca del ciberacoso escolar y la seguridad en Internet, y la National Cyber Security Alliance ha creado un magnífico sitio web (StaySafeOnline.org) y ha puesto en funcionamiento otra programación pública para formar a nuestra sociedad digital en el uso de Internet de una manera segura, ya sea desde el hogar, el trabajo o la escuela. Con todo, estos esfuerzos deben ampliarse enormemente para poder hacer frente al siguiente nivel de amenazas que se cierne sobre nosotros a través de un amplio despliegue de avances tecnológicos, como la Internet de las Cosas. Tal como se ha indicado previamente, la gran mayoría de estas amenazas tecnológicas deben gestionarse desde un nivel sistémico, pero las personas también tenemos que entender que los riesgos que entrañan y responsabilizarnos de protegernos y de proteger a nuestras familias en la medida de lo posible. La necesidad de educación es tan grande en el sector privado como en el empresarial. También las empresas sufren ataques, y no sólo por parte de Crimen, S. A., sino por sofisticados servicios de espionaje de Estados nación que persiguen la propiedad intelectual y los datos corporativos. Las medidas de seguridad que por tradición sólo tenían que aplicarse en las organizaciones de máximo secreto son hoy una necesidad imperiosa para todo el mundo empresarial. Y en este campo los recursos educativos también son profundamente limitados, una situación que debemos abordar si queremos progresar frente a las amenazas tecnológicas que nos aguardan.

El factor humano: el eslabón débil olvidado

> Si crees que la tecnología puede solucionar tus problemas de seguridad, entonces es que no entiendes ni los problemas ni la tecnología.
>
> BRUCE SCHNEIER

La ciberseguridad es un problema que tenemos, y no sólo técnico. Al margen del nivel de fortaleza que tenga tu contraseña informática, si la escribes en una notita amarilla adhesiva y la pegas a la pantalla de tu ordenador para no olvidarla, cualquiera que pase por delante tendrá acceso a tu vida digital. En el caso de las decenas de miles de personas que pierden dinero en la estafa del príncipe nigeriano cada año, su problema no es técnico, sino el atributo humano omnipresente de la

esperanza y la avaricia. Y si publicas tus planes para las vacaciones en las redes sociales y los ladrones hacen una visitita a tu domicilio, fue tu decisión de compartir lo que facilitó su actividad delictiva. Y por cada persona que hace clic en ese enlace del banco que le dice que su contraseña ha caducado y debe cambiarla, el desafío en sí no es que le hayan pirateado el ordenador, sino que ha sido víctima de un ataque de *phishing* urdido mediante ingeniería social. Por muchos cortafuegos, tecnologías de encriptación y programas antivirus que utilice una empresa, si el ser humano sentado tras el teclado cae en una trampa, la empresa está vendida. De acuerdo con un estudio en profundidad realizado en 2014 por los Servicios de Seguridad de IBM, hasta el 95 por ciento de los incidentes de seguridad se debían a un error humano[14]. El factor humano puede inhabilitar todas las medidas de seguridad tecnológicas, por lo que es clave tanto la formación personal como la de la plantilla.

Tal como se ha mencionado en el prólogo, la tecnología puede efectivamente protegernos. La autenticación multifactor, la biometría, la encriptación y la geolocalización pueden poner freno a la delincuencia y reducir otros riesgos a la seguridad. Ahora bien, tal como hemos visto en reiteradas ocasiones, estas herramientas tecnológicas pueden socavarse. Sin duda alguna, la NSA tenía a su disposición herramientas de ciberseguridad punteras y, sin embargo, fue un ser humano, Edward Snowden, quien las subvirtió antes de huir con multitud de datos clasificados en su unidad USB. Y lo mismo se aplica con relación a la central nuclear «pacífica» iraní en Natanz, que implementaba sólidas medidas de seguridad y no tenía conectados a Internet sus sistemas de control industrial. Con todo, estas medidas fueron derrotadas fácilmente cuando alguien desconocido insertó sin pensárselo una unidad USB infectada en un ordenador de sobremesa de la instalación. Aquella decisión desinformada permitió que el gusano Stuxnet se propagara por la red interna responsable de controlar las centrifugadoras de uranio de las instalaciones. Siempre conviene recurrir a una solución tecnológica fácil cuando surge un problema, pero los empresarios, los legisladores, las empresas de Internet y los programadores informáticos deben tomar en consideración la dimensión humana de la seguridad si desean evitar riesgos tecnológicos tanto presentes como futuros.

La buena noticia es que podemos modificar nuestro comportamiento humano para mejorar de manera significativa nuestra seguridad tecnológica digital. Para contextualizar este aspecto, resulta útil compararlo con los robos de coches. Si el propietario de un BMW aparcara su vehículo en un barrio plagado por la delincuencia, las decisiones personales que adoptara acerca de la seguridad del automóvil repercutirían enormemente en la probabilidad de que lo robaran o no. Si él aparcara en una zona bien iluminada, cerrara todas las puertas y ventanas y activara la alarma, habría adoptado todas las medidas razonables para evitar que le robaran el coche. Con el tiempo, la mayoría de nosotros hemos aprendido que así es exactamente como debemos proteger nuestros vehículos. En cambio, la mayoría de la población no tiene ni idea de cómo desplegar un comportamiento similar en el

ciberespacio. Y, en consecuencia, nos conectamos a la Red y aparcamos virtualmente nuestros vehículos en callejones oscuros y aislados, nos dejamos las puertas y ventanas abiertas, no activamos la alarma, nos olvidamos las llaves puestas y, además, dejamos billetes de cien dólares a la vista en el asiento del copiloto. Y luego nos preguntamos cómo es posible que nos hayan robado el coche.

El objetivo aquí no es perseguir a un unicornio esquivo llamado «seguridad perfecta», sino mejorar de manera palpable la situación actual. Una vez más, el ejemplo del BMW nos puede resultar instructivo. Incluso al conductor que tomó todas las medidas y precauciones correctas para protegerse y proteger su vehículo podrían robarle el coche. Un delincuente podría pasar por allí con un camión de plataforma o una grúa y llevarse el coche, o simplemente forzar las puertas y hacerle el puente al motor. Con tiempo, energía, atención y recursos suficientes, cualquier sistema puede manipularse. El objetivo no es lograr una seguridad perfecta, sino entender cómo bloquear las puertas y ventanas de tu vehículo en el ciberespacio y, en este sentido, tienes muchas herramientas a tu disposición. Pese a ello, muchas de las decisiones arriesgadas que has tomado hoy durante tu navegación por Internet no son culpa tuya, sino del diseño lamentable de los sistemas informáticos, tanto *software* como *hardware*, sitios web y teléfonos inteligentes. Es hora de solucionarlo.

Incorporación del diseño humano en la seguridad

> Cuando planteas con empatía un proceso de resolución de problemas creativo al público, se multiplican las oportunidades de innovar.
>
> TOM KELLEY, IDEO

¿Por qué no actualizan la contraseña los clientes? ¿Acaso son tontos? ¿Por qué no utilizan redes personales virtuales (VPN) y cortafuegos? ¿Qué utiliza WEP o WPA2?

Como sabe cualquiera que haya telefoneado alguna vez al departamento de asistencia técnica para que le solucionen un problema informático, la mayoría de los administradores de sistema y el personal de atención al público no tiene a sus «clientes» en una particularmente alta estima. El diagnóstico más habitual que emite el personal del departamento técnico es que el problema está en la silla, no en el ordenador. Para quienes han estudiado ciencia informática, han tomado clases de criptografía y han soñado con código PHP y C++, hablar con el usuario informático medio puede ser un proceso frustrante. Literalmente, hablamos dos idiomas distintos. Para los ingenieros en materia de seguridad, las respuestas parecen evidentes: «Si los malditos usuarios dejaran de hacer la estupidez *x* o *y*, todo funcionaría como la seda». Al otro lado de la línea, los usuarios tienen una única pregunta que suelen guardarse para sí: «¿Por qué no te limitas a darme instrucciones sencillas y me permites

reincorporarme a mi trabajo?». Las herramientas de seguridad de las cuales disponemos hoy son demasiado complejas y farragosas de utilizar y no nos engañemos: la complejidad es enemiga de la seguridad.

Los arquitectos de la seguridad de la información hablan en jerga acerca de virus, *malware*, días cero, *exploits*, vulnerabilidades, troyanos, RAT y AES, y, en su inmensa mayoría, el público en general no tiene ni idea de qué le están diciendo. El *software* de seguridad y los productos de *hardware* actuales están diseñados, de manera casi invariable, por entendidos en informática para entendidos en informática. No hay ni un pensamiento pasajero ni una pizca de empatía hacia cómo utilizarás tú esas herramientas, por no hablar ya de cómo las utilizará tu abuela. En su lugar, los productos concebidos para brindarnos seguridad y protegernos nos muestran útiles mensajes de advertencia como: «Alerta: Un proceso host para Windows Service que utiliza protocolo UDP saliente, IPv6NAT Traversal-No, está intentando acceder a Internet. ¿Deseas continuar?». ¿Qué demonios significa eso? Nadie lo sabe, salvo los creadores de esta advertencia tan «útil». Ha llegado el momento de incorporar un diseño amable y fácil de entender por el usuario al mundo de la ciberseguridad.

Piensa en el diseño de un iPhone 6, de un sillón Eames, de un Ferrari 458 Italia o de una cámara Leica T, productos concebidos para deleitar. No sólo son herramientas funcionales, sino que además son bellas y están creadas por personas que entendían perfectamente a sus clientes y sus necesidades. Cuando uno observaba a Steve Jobs en el escenario presentar sus últimos productos, no cabía ninguna duda de que todos y cada uno de ellos rezumaba el amor con el que lo habían creado. Entonces ¿dónde está el Steve Jobs de la seguridad? ¿Qué puede el diseñador jefe de Apple, Jony Ive, aportar al problema de la creciente ciberinseguridad? ¿Qué aspecto tendrían sus programas cortafuegos o antivirus? Hasta el momento, no tenemos ni idea, y es un problema colosal.

Es un problema porque, cuando las funciones de seguridad no están bien diseñadas, la gente sencillamente prescinde de usarlas. Es más, un diseño pobre puede conducir a los usuarios humanos por sendas que los hacen aún más vulnerables. ¿Por qué anotan las personas las contraseñas en notas *Post-it* y las pegan a sus ordenadores? Porque obligarlas a cambiarlas cada dos semanas y exigirles que tengan como mínimo veinte caracteres de longitud, con una letra en mayúsculas, un número, un símbolo, un haiku y un pentámetro yámbico sencillamente excede las capacidades del usuario estándar. De manera que las personas subvierten los sistemas de seguridad activos para poder trabajar. Existen también algunos tipos de productos de seguridad, como los programas cortafuegos, que emiten tantas alertas falsas que el usuario acaba por desactivarlos para evitar ver constantes ventanas emergentes con mensajes de advertencia incomprensibles. En estos casos, cuando se produce alguna brecha en la seguridad, el personal del departamento de TI culpa invariablemente al usuario. Quizá convendría mirarse al espejo primero. Vaya por delante que los diseñadores de productos y sistemas de seguridad no son personas ni insensibles ni

ignorantes, simplemente están a años luz de entender las necesidades de sus clientes. Tomando prestada una frase, ha llegado el momento de «pensar diferente».

El diseño de productos antropocéntricos es fundamental para impulsar los cambios de conducta que precisamos en el ámbito de la tecnoseguridad y para minimizar el número creciente de amenazas que afrontamos. Los diseñadores de estos productos necesitan entender humanamente cómo interactúan las personas con los ordenadores y los teléfonos móviles, en lugar de esperar que sean los usuarios quienes se amolden a comportamientos extraños o entiendan avisos de pantalla esotéricos. Hasta que los gurús de la seguridad no empiecen a crear productos que el público general pueda entender y poner en práctica, la población carecerá de las herramientas y de la información que precisa para protegerse. Y si bien los programas educativos ampliados y el diseño antropocéntrico sin duda pueden conllevar una mejora sustancial en el estado general de la seguridad técnica hoy en día, algunas amenazas exceden la capacidad de una sola persona de reaccionar. En tales casos es preciso aplicar una serie de cambios sistémicos, y tanto la naturaleza como la medicina pueden proporcionar una inspiración útil sobre cuál es el mejor camino para seguir avanzando.

La Madre Naturaleza es sabia: dotemos a Internet de un sistema inmunitario

En la actualidad, las ciberamenazas evolucionan tan rápidamente que nuestras barreras defensivas no dan abasto a contenerlas. No sólo tenemos a los bárbaros proverbiales a las puertas, sino que las derriban y reptan por todo el castillo. Precisamos métodos defensivos más robustos, reactivos y flexibles, algo similar al sistema inmunitario humano. En los más de tres mil millones de años desde que hay vida en el planeta, millones de especies distintas, incluidos los seres humanos, han aprendido a bregar con un abanico innumerable de amenazas. A los animales, un sistema inmunitario adaptativo nos protege de diversos patógenos ajenos, como virus, parásitos, bacterias e incluso toxinas ambientales. Los diseños que vemos a nuestro alrededor en la naturaleza pueden servir de magnífica fuente de inspiración en nuestros intentos por solventar problemas humanos complejos, y existe todo un campo de estudio dedicado justo a este desafío: la llamada biomimética. A título de ejemplo, los científicos estudian en estos momentos cómo procesan las hojas la energía solar para inventar placas solares mejores. Entonces, ¿por qué no buscar en la naturaleza la inspiración para innovar en la creación de redes informáticas con capacidad de autosanar?

Hasta ahora, nuestra manera habitual de enfocar la ciberseguridad ha sido

protegernos con muros frente a las posibles amenazas tecnológicas, pero no conectarse a Internet o no usar las tecnologías sencillamente no es una opción sobre la mesa. Un planteamiento mucho más adecuado sería identificar los riesgos y adaptarse rápidamente a ellos, según se vayan presentando, tal como hace nuestro sistema inmunitario. El sistema inmunitario humano no se defiende contra una única cepa de gripe, sino que se adapta rápidamente y aprende a bregar con todo el espectro de cepas. Esto es posible porque el cuerpo entiende maravillosamente qué constituye lo «propio» y saludable frente a lo «ajeno» y peligroso[15]. Con todo, tales planteamientos son, a lo sumo, rudimentarios en los sistemas de tecnodefensa actuales. Tanto DARPA como el Pacific Northwest National Laboratory han lanzado proyectos en la materia, y uno de los enfoques más interesantes ya está en marcha en la Wake Forest University. Allí, el profesor de ciencias informáticas Errin Fulp utiliza la inteligencia natural para formar enjambres de las colonias de insectos para formar barreras frente a ciberdepredadores desplegando miles de programas de *software* a modo de «hormigas digitales» por toda una red informática, cada uno de los cuales busca señales de amenaza. En el caso de detectarse una de estas amenazas, la hormiga digital marca el problema con el equivalente a una fragancia virtual y atrae al resto de las hormigas. Los rastros de fragancias más potentes atraen más hormigas digitales, que acaban plagando cualquier infección informática en potencia antes de que se desmadre[16]. La velocidad de propagación de las ciberamenazas es tan rápida que es imposible que los seres humanos las contengamos. Del mismo modo, nuestro objetivo debería ser crear distintos sensores e implantarlos en las redes mundiales no sólo para detectar a nuevos intrusos y averiguar cómo se han colado en ellas, sino, lo que es más importante, para efectuar las reparaciones necesarias de manera automática, una red capaz de autosanarse que no requiera intervención humana para repararse. Un sistema inmunitario para el planeta. Hasta que tal sistema exista, concentraremos nuestros esfuerzos en enfoques mucho más centrados en el capital humano para solucionar el problema, como utilizar a los cuerpos de seguridad para arrestar a los depredadores.

Patrullar el siglo XXI

> En un mundo caracterizado por los cambios impulsados por la tecnología, la única opción es legislar tras los hechos y bregar a perpetuidad por estar al día.
>
> WILLIAM GIBSON

No es fácil patrullar la Red. Nos llegan noticias de que la supuestamente omnipotente NSA lleva un seguimiento de todos nuestros movimientos en el ciberespacio y es indudable que la Agencia se ha dotado de un imponente despliegue de herramientas y

técnicas. Pero, para el agente de policía o el detective de a pie, Internet es un lugar difícil donde actuar. Los policía de la División 77 del Departamento de Policía de Los Ángeles (LAPD), el distrito policial Midtown South del Departamento de Policía de Nueva York y el distrito de Englewood de Chicago no tienen acceso a ninguna de las herramientas empleadas por los organismos de espionaje; esa información está clasificada y es demasiado sensible para exponerla ante un juez. Incluso en organizaciones como el FBI se deben salvar barreras importantes a la hora de llevar a cabo investigaciones de casos de ciberdelincuencia, sobre todo en el extranjero. A nivel estatal, local y federal, los agentes de los cuerpos de seguridad se encuentran sobrepasados de manera crónica y acusan una grave carestía de personal, tal como ha puesto en evidencia el crecimiento explosivo de la delincuencia en Internet detallado en este libro. Las pérdidas anuales de cuatrocientos mil millones de dólares que se calcula que sufre la economía mundial a causa de la ciberdelincuencia demuestra simple y llanamente que la policía está perdiendo la guerra contra Crimen, S. A. de manera estrepitosa.

Los atacantes, gracias a los pingües beneficios que les proporcionan sus aventuras en la clandestinidad digital, suelen aprovechar las tecnologías mucho antes de que los cuerpos de seguridad y los investigadores puedan hacerlo. Disponen de presupuestos prácticamente ilimitados y no tienen que lidiar con burocracias internas, procesos de aprobación ni restricciones legales. Sin embargo, hay otros temas sistémicos que dan ventaja a los delincuentes, en concreto la jurisdicción y la legislación internacional. En cuestión de minutos, el artífice de un delito en Internet puede visitar virtualmente seis países distintos, saltando de servidor en servidor y de continente en continente en un instante. En cambio ¿qué sucede con la policía que tiene que seguir el rastro de pruebas digitales para investigar el asunto? Pues lo tiene mucho más difícil. Como sucede con todas las actividades gubernamentales, políticas y procedimientos, hay que seguir una determinada normativa. Los ciberataques transfronterizos plantean serios problemas jurisdiccionales, no ya sólo a un departamento policial concreto, sino a la institución de la policía en su conjunto tal como está formulada actualmente. Un agente de Dallas no esta autorizado a obligar a un proveedor de servicios de Internet (ISP) de Tokio a que le proporcione pruebas, ni puede realizar arrestos en el distrito de Ginza. Eso es algo que sólo puede hacerse por solicitud, de gobierno a gobierno, a menudo mediante tratados de asistencia legal mutua. El ritmo terriblemente lento del derecho internacional implica que normalmente transcurren varios años antes de que la policía reciba al fin pruebas de ultramar (años en un mundo en el que las pruebas digitales pueden destruirse en segundos). Peor aún, la mayoría de los países aún no disponen de leyes que regulen la ciberdelincuencia, lo cual redunda en que los delincuentes pueden actuar con total impunidad. Y tal y como hemos visto con los narcotraficantes y los blanqueadores de dinero, los ciberdelincuentes son lo suficientemente listos como para ampararse en países refugio.

El derecho penal es nacional, lo cual conlleva que se respeta la soberanía de cada país para establecer sus propias leyes y regulaciones sin injerencia externa en sus asuntos internos, y se remonta al Tratado de Westfalia de 1648. Si bien este sistema funcionó bien durante siglos, actualmente está sometido a una presión implacable y creciente a causa de una Internet global que está erosionando tales fronteras. El legado del Tratado de Westfalia es una respuesta geográfica a un problema no geográfico. La amenaza tecnológica que afrontamos no conoce fronteras y, por consiguiente, sólo puede gestionarse mediante una reacción internacional apropiada. Una institución como la Interpol, la Organización Internacional de Policía Criminal, tiene un papel importante que desempeñar en la lucha contra la ciberdelincuencia transnacional y en la coordinación de las investigaciones entre sus 190 países miembro. El problema es que la Interpol cuenta con un presupuesto operativo de sólo noventa millones de dólares para combatir al conjunto de la delincuencia internacional, desde el tráfico de personas hasta los robos de arte. En comparación, sólo el NYPD maneja un presupuesto de 4900 millones de dólares y un único delincuente, el líder del narcotráfico mexicano Joaquín «El Chapo» Guzmán Loera guardaba casi doscientos millones de dólares en efectivo en su domicilio cuando fue arrestado (más del doble del presupuesto anual de la Interpol). Las investigaciones criminales, en especial las que abarcan múltiples jurisdicciones e inmensas cantidades de pruebas electrónicas, no sólo requieren un trabajo ingente sino que son excepcionalmente caras. Si no se amplía sensiblemente el presupuesto de la policía para afrontar estos problemas, debemos prepararnos para que Crimen, S. A. prosiga sin cese en sus empresas ilegales.

Con todo, ni siquiera un incremento a gran escala en los recursos de los cuerpos de seguridad resolvería el problema de las ciberamenazas, sino que hay un componente cultural en nuestro sistema de justicia penal que debe abordarse también. En 2012, Janet Napolitano, la secretaria del Departamento de Seguridad Nacional de Estados Unidos a la sazón, admitió que no utilizaba ni el correo electrónico ni otros servicios en línea «para nada»[17]. Correcto: el máximo responsable gubernamental de la ciberseguridad y la protección de las infraestructuras básicas de Estados Unidos no utilizaba el correo electrónico…, pero no por motivos de seguridad, sino porque, según ella misma confesó, era «un poco ludita». En 2013, la magistrada del Tribunal Supremo de Estados Unidos admitió que los jueces «no son las personas tecnológicamente más sofisticadas que existen» y que «en la corte aún no se utiliza el correo electrónico»[18]. En su lugar, explicó, «nos comunicamos mediante memorándums internos impresos en papel marfil que los secretarios del juzgado entregan en mano». Pese a que es indudable que los magistrados y secretarios de gabinete que trabajan en las instancias más elevadas del sistema judicial penal poseen imponentes intelectos, su aparente falta de interés y dominio de tecnologías incluso rudimentarias es digna de destacar. En un mundo que avanza a un ritmo tan acelerado, ¿cómo es posible que personas que no utilizan el correo electrónico

legislen sobre ciberseguridad, tecnología y privacidad?

Los elementos nucleares de nuestro sistema de justicia deben estar mínimamente versados en el lenguaje de la ciencia y la tecnología. Los investigadores no sólo deben entender cómo funcionan estas herramientas, sino ser tan creativos como aquéllos a quienes persiguen…, algo prácticamente imposible habida cuenta de la burocracia con la que delegan los cuerpos de seguridad. Así, mientras que los delincuentes utilizan la inteligencia artificial para ejecutar *scripts* y automatizar delitos, la policía responde a cada delito manualmente. La delincuencia muda de piel, pero los cuerpos de seguridad no: tenemos robots delincuentes dotados de IA, pero ¿dónde están los robots policías dotados de IA para combatirlos? ¿Dónde se registra ese nivel de innovación en el gobierno? Necesitamos un Departamento de Científicos Locos en el FBI, un cuadro de mandos de agentes especiales que no luzcan camisas blancas almidonadas y corbata, pero sí desplieguen una creatividad para la piratería informática similar a las de sus oponentes. Deberían ser piratas con ética[*] extraídos de todos los estamentos de las sociedad y con un pensamiento fuera de lo común. Espoleemos la creatividad y la innovación entre ellos tal como hace Google, con un programa laboral con un 20 por ciento de tiempo libre que permita a los agentes investigar proyectos especiales un día a la semana, liberados de las tareas que se les asignan a diario. Cuando Google anunció públicamente sus planes, sus fundadores mencionaron que ese 20 por ciento del tiempo era fundamental para la capacidad de la empresa de innovar y añadieron que había conducido a «muchos de nuestros progresos más destacados», incluidos Gmail, Google Talk, Google News y AdSense (en la actualidad responsable del 25 por ciento de los ingresos de la empresa). La mayoría de los organismos de los cuerpos de seguridad están tan ocupados que sólo tienen tiempo de concentrarse en el aspecto táctico que tienen delante de los ojos, lo cual apenas les deja tiempo para aplicar el importantísimo pensamiento estratégico necesario para solucionar el problema. Por mucho que gastemos en patrullar, nunca seremos capaces de acorralar el problema de la ciberdelincuencia.

La necesidad de adoptar nuevos planteamientos es imperiosa, dado que nuestros sistemas de jurisdicción y justicia *offline* pueden ser fundamentalmente incompatibles con nuestro mundo online en constante expansión. Por ejemplo, hay departamentos policiales que se ocupan del ciberespacio, pero ¿dónde están los ciberbomberos, tal como ha preguntado con gran criterio el pionero de Internet Vint Cerf? Cuando la casa de tu vecino se incendia y amenaza la tuya, el objetivo no debería ser arrestar a tu vecino por «incendio provocado», sino evitar que la tuya se queme. Y mientras que los cuerpos de seguridad sirven perfectamente para ocuparse de asuntos criminales, es posible que otras opciones distintas funcionaran mejor para abordar la montaña creciente de ciberamenazas. En concreto, ha llegado el momento de concentrarse en la prevención en lugar de en la investigación retrospectiva y en tratar el problema después del hecho. En este aspecto, tenemos mucho que aprender del mundo de la sanidad pública mientras bregamos por mitigar los riesgos de nuestra inseguridad

tecnológica.

Tecnología segura: la necesidad de una buena ciberhigiene

Todos sabemos qué aspecto luce la buena higiene en el mundo físico. Y nos insisten en que la practiquemos. En los aseos de los restaurantes, los carteles recuerdan a los empleados que deben lavarse las manos antes de reincorporarse al trabajo. Tu madre te dice que te tapes la boca al estornudar y colegas, médicos y vallas publicitarias por doquier nos recuerdan que utilicemos condones y practiquemos sexo seguro. Pero ¿dónde están estos mensajes en el mundo virtual? Mamá no nos recuerda que no aceptemos unidades USB de extraños y conectamos de manera rutinaria estos dispositivos transmisores de virus en nuestro ordenadores, a raíz de lo cual participamos, sin saberlo, en la propagación de *software* malicioso e infectamos a nuestros vecinos y amigos. Y el hecho de no vacunar mi propia tecnología implica que, cuando me infecto y me convierto en un esclavo del Borg criminal, participo sin ser consciente en ataques DDoS y estafas de *phishing* a otras personas.

La salud de Internet, como la salud pública, es una responsabilidad compartida y los internautas deben administrar sus redes y dispositivos si queremos mejorar la seguridad en el futuro tecnológico. Tenemos la obligación moral de hacerlo. Cada uno de nosotros debe ser un buen pastor de su rebaño tecnológico y proteger sus ordenadores, teléfonos y otros dispositivos para no causar perjuicios a terceros. La buena noticia es que practicar una buena higiene virtual es mucho más sencillo de lo que parece, para lo cual he incluido una lista de técnicas sencillas en el apéndice de este libro que pueden reducir drásticamente el riesgo de ciberamenazas. Si bien circulan multitud de listas de mejores prácticas extensas y complejas, el gobierno australiano las redujo de manera brillante a sólo cuatro estrategias clave[19]:

- Lista blanca de aplicaciones: ejecuta sólo los programas específicamente autorizados en tu sistema y bloquea todos los archivos ejecutables y rutinas de instalación. De esta manera evitarás que se ejecuten *software* malicioso y aplicaciones dañinas.
- Aplica los parches a todas las aplicaciones de los dispositivos ejecutando de manera automática las actualizaciones de *software* para programas como MS Office, Java, lectores de PDF, *Flash* y navegadores web.
- Aplica los parches a las vulnerabilidades de los sistemas operativos (OS) actualizando automáticamente el OS como Windows, Mac, iOS o Android, lo cual te garantizará que utilizas la última versión del sistema operativo en todo

momento.

- Limita los privilegios como administrador en tu ordenador y pasa la mayor parte del tiempo conectado como un usuario básico, en especial cuando trabajes con el correo electrónico o navegues por Internet. Conéctate sólo como administrador de tu propia máquina cuando precises hacerlo, como para instalar *software* nuevo o efectuar cambios en el sistema. De este modo privas a los adversarios de los privilegios como administrador que suelen necesitar para instalar *software* malicioso y rebuscar en tu red.

La mera adopción de estos cuatro sencillos pasos mitiga la asombrosa cifra del 85 por ciento de las intrusiones dirigidas, según las investigaciones llevadas a término por el gobierno australiano. Un estudio en profundidad realizado por Verizon y los servicios secretos estadounidenses revelaron unas noticias igual de positivas: «el 97 por ciento de todas las filtraciones de datos podrían haberse evitado aplicando controles de un nivel sencillo o intermedio»[20]. Un mejor diseño de los productos tecnológicos y una superior educación pública pueden ayudarnos a recorrer un largo camino elaborando con las personas y las empresas por igual para que adopten las decisiones correctas en lo tocante a ciberhigiene. No obstante, para afrontar las amenazas restantes y las más persistentes, se precisa un enfoque más global y unificado, inspirado en los modelos de la epidemiología y la propagación de enfermedades.

El Centro Virtual para el Control y la Prevención de Enfermedades: la Organización Mundial de la Salud para un Planeta Conectado

El lenguaje de la inseguridad técnica está plagado de metáforas de la enfermedad. Hablamos de virus informáticos e infecciones para describir el código malicioso que se autorreplica, pero, en lugar de concentrarnos en la prevención y en la detección, solemos culpar a aquellos que han sido infectados e intentamos arrestar y juzgar retrospectivamente a los responsables mucho después de ocasionado el daño. ¿Qué sucedería si cambiáramos este paradigma y, en su lugar, contempláramos la ciberseguridad común como un ejercicio de salud pública? Organizaciones como los Centros para el Control y la Prevención de Enfermedades de Atlanta y la Organización Mundial de la Salud de Ginebra han desarrollado en el transcurso de varias décadas sistemas robustos y metodologías objetivas para identificar y responder a amenazas a la salud pública, estructuras y marcos mucho más desarrollados que los de la comunidad de la seguridad virtual. Teniendo en cuenta los

múltiples paralelismos entre las enfermedades humanas comunicables y las que afectan a las tecnologías del mundo, nos queda mucho por aprender del modelo de salud pública, un sistema adaptable para reaccionar a una serie de patógenos mutantes en todo el mundo.

Cabe destacar que, en asuntos de salud pública, las acciones individuales tienen una repercusión limitada. Es fantástico poner en práctica técnicas excelentes de higiene personal, pero, si vives en una población con ébola, tarde o temprano también sucumbirás. La comparación es relevante para el mundo de las amenazas virtuales. La responsabilidad y las acciones individuales pueden suponer una diferencia inmensa en la ciberseguridad, pero, en última instancia, la única esperanza que tenemos para reaccionar a las amenazas que se propagan a gran velocidad por esta matriz planetaria de tecnologías interconectadas es fundar nuevas instituciones que coordinen nuestra respuesta. Una Organización Mundial de la Salud virtual e internacional podría fomentar la cooperación y colaboración entre empresas, países y organismos gubernamentales, pasos esenciales e imprescindibles para mejorar la salud pública de las redes que gobiernan las infraestructuras críticas tanto en el mundo en línea como fuera de línea.

Un Centro de Control y Prevención de Enfermedades (CCPE) virtual podría ser de gran ayuda para contrarrestar los riesgos tecnológicos que afrontamos en la actualidad y podría desempeñar un papel fundamental en la mejora de la salud pública general de las redes que operan las infraestructuras esenciales del mundo. En efecto, un informe patrocinado por Microsoft y el EastWest Institute sugería que un CCPE podría ejercer múltiples papeles que en la actualidad sólo se aplican de manera específica, *ad hoc*, incluidos entre ellos los siguientes[21]:

- educación: proporcionar al público métodos de higiene virtual de eficacia demostrada para protegerse;
- supervisión de redes: detección de infecciones y brotes de *software* malicioso en el ciberespacio;
- epidemiología: aplicar metodologías propias de la salud pública para estudiar la propagación de enfermedades digitales y ofrecer pautas para responder a ellas y remediarlas;
- inmunización: contribuir a vacunar al público frente a amenazas conocidas usando parches de *software* y actualizaciones de sistema, y
- respuesta a incidentes: enviar a expertos cuando sea preciso y coordinar los esfuerzos mundiales por aislar el origen de las infecciones en línea y ofrecer tratamiento a los afectados.

Si bien existen múltiples organizaciones, tanto gubernamentales como no gubernamentales, que se ocupan de desempeñar todas estas tareas, no existe una única entidad que las abarque todas. Y precisamente a través de estas brechas en la

coordinación y los esfuerzos conjuntos continúan multiplicándose los ciberriesgos. En concreto, es preciso adoptar un planteamiento epidemiológico frente a los riesgos tecnológicos crecientes para llegar a la fuente de las infecciones de *malware*, como sucedió en la lucha contra la malaria. Durante décadas, todos los esfuerzos médicos se concentraron en vano en tratar esta enfermedad parasitaria mortal en los pacientes ya infectados. Hasta que los epidemiólogos no cayeron en la cuenta de que la enfermedad la propagaban los mosquitos que bebían en aguas estancadas no se avanzó realmente en la lucha contra la malaria. Al drenar las ciénagas donde proliferan los mosquitos y sus larvas, los epidemiólogos los privaron de un importante caldo de cultivo y redujeron el contagio de la malaria. ¿Qué ciénagas podemos drenar en el ciberespacio para conseguir unos resultados similares? Aún no lo hemos determinado; de ahí la importancia de esta obra.

Ahora bien, los CCPE afrontarían otro gran desafío: la mayoría de los enfermos desconocen que están infectados y contagian la enfermedad. Mientras que los pacientes de malaria experimentan fiebres, sudores, náuseas y dificultades respiratorias, síntomas manifiestos de su enfermedad, los virus informáticos pueden ser completamente asintomáticos. Esta diferencia trascendental queda en evidencia por el hecho de que la abrumadora mayoría de las personas con dispositivos infectados no tienen ni idea de que sus máquinas encierran *software* malicioso ni de que han pasado a formar parte de un ejército de *botnets*. Incluso en el mundo corporativo, donde el tiempo medio de detección de una intrusión en una red se sitúa actualmente en 210 días, la mayoría de las empresas no saben que sus activos más valiosos, ya sean propiedad intelectual o la maquinaria de su fábrica, han sido vulnerados.

Lo único peor de que te pirateen es que te pirateen y no te des cuenta. Si no sabes que estás enfermo, ¿cómo vas a conseguir tratamiento? Es más, ¿cómo podemos prevenir la propagación de las enfermedades digitales si los portadores de dichas enfermedades no saben que están contagiándolas? Abordar estos temas será un área de importancia trascendental para cualquier Organización Mundial de la Salud virtual que se proponga y fundamental para la seguridad comunitaria del futuro y para la de nuestras infraestructuras de información básicas.

El investigador en materia de ciberseguridad Mikko Hypponen ha señalado cuál es el talón de Aquiles evidente del mundo moderno poblado de tecnología en el que vivimos: el hecho de que todo funcione con ordenadores y que todo dependa de que esos ordenadores funcionen. El desafío que tenemos por delante es que, de alguna manera, tenemos que continuar trabajando aunque todos los ordenadores fallen. Si nuestros sistemas de información dejaran de funcionar a escala masiva, se cerrarían los mercados financieros, lo cajeros automáticos no darían dinero, no habría red telefónica ni gasolina. Si estos pilares de nuestra sociedad desaparecieran de repente, ¿cuál sería el plan B de la humanidad? La respuesta es muy sencilla: no tenemos plan B.

Dar los pasos esbozados en este capítulo nos permitiría avanzar un buen trecho hacia la protección de la multitud de amenazas que afrontamos hoy en día, pero este plan de actuación dista mucho de ser infalible. Nos hallamos en el amanecer de la carrera armamentística tecnológica, una carrera armamentística entre personas que utilizan la tecnología para bien y otras que la utilizan para mal. El desafío es que los usos viles de la tecnología se multiplican exponencialmente de modos que nuestros actuales sistemas de protección no consiguen frenar. Ha llegado el momento de dotar de una mayor resiliencia a la red de comunicación global para evitar que el sistema falle. Si queremos sobrevivir al progreso que nos ofrecen las tecnologías y disfrutar de su munificencia, primero debemos idear mecanismos de seguridad adaptables que igualen o superen la velocidad exponencial de las amenazas. Y en ésta, nuestra principal misión, sobran todas las ambigüedades: no hay tiempo que perder.

Capítulo 18

El camino por delante

> Que a nadie le desaliente la idea de que no hay nada que podamos hacer frente a las enfermedades, la miseria, la ignorancia y la violencia que pueblan nuestro mundo. Pocos tendrán la grandeza de cambiar el rumbo de la historia, pero cada uno de nosotros puede aportar su pequeño grano de arena para cambiar el curso de los acontecimientos. Y, en total, la suma de esos granos será la historia escrita de una generación.
>
> ROBERT F. KENNEDY

Ya no podemos volver a meter en la lámpara al genio tecnológico. Tanto en los campos de lo virtual, la robótica, la inteligencia artificial y la biología sintética hay cambios trascendentales en marcha en este mundo. Y dichos cambios nos han conducido hasta la rodilla de una curva exponencial, la cual registrará un crecimiento explosivo en los años venideros. De hecho, estos grandes avances se producirán mucho antes de lo que la mayoría sospecha, ya que un ámbito científico fomenta el progreso en otros. Los avances en la tecnología de la información impulsan la biología sintética y la inteligencia artificial espolea la robótica. Estas fuerzas se influyen recíprocamente y provocan exponenciales de exponenciales. No obstante, tal como se ha descrito a lo largo de este libro, no todos estos avances serán para bien. Ejemplo tras ejemplo, hemos documentado cómo los delincuentes, terroristas, piratas informáticos y gobiernos corruptos subvierten la tecnología y la emplean en perjuicio de otros. Por supuesto, ello no quiere decir en ningún caso que la tecnología sea mala. El fuego, la primera tecnología, servía para dar calor, para cocinar alimentos y también para incendiar y reducir a cenizas el pueblo vecino. Y tanto un cirujano como un asesino pueden blandir un cuchillo. En manos de las personas con buenas intenciones, las tecnologías, que evolucionan rápidamente, aportarán una abundancia sensacional al mundo. Pero, en manos de un hombre-bomba, el futuro puede antojarse muy distinto.

Fantasmas en la máquina

> Medir es saber.
>
> LORD KELVIN

Uno de los principales desafíos que afrontamos a causa de la falta de seguridad tecnológica actual es que, con frecuencia, las intrusiones informáticas en nuestras redes o dispositivos dan muy pocas señales, si es que dan alguna. El problema evidente es que se tienen invitados no deseados (tanto si uno se da cuenta como si no). Pero el mayor problema es que resulta imposible combatir algo que no se ve. En nuestros teléfonos inteligentes, ordenadores portátiles, tabletas, cuentas bancarias, frigoríficos, vehículos, redes corporativas y tendidos eléctricos hay fantasmas. Mantener a raya a todos los intrusos en todo momento era un objetivo noble aunque pintoresco. Pero, por si no te has dado cuenta, la proverbial república tecnológica ha fracasado. Nuestra tecnología está repleta de errores, fallos e invasores. Por desgracia, nuestro objetivo hoy ya no puede ser únicamente la prevención. Debemos perseguir a los fantasmas que se han colado en nuestras máquinas buscándolos de manera proactiva y dándoles caza. Con un tiempo de detección que supera los doscientos días, está claro que nos queda mucho camino por delante. Necesitamos reducir ese marco temporal a unas pocas horas, hasta conseguir limitarlo a cuestión de minutos y segundos.

Y luego está el problema persistente de los datos masivos: cuantos más conservemos, más debemos proteger. Ocurre que la mayoría de las empresas nunca han catalogado sus activos informativos y, por ende, no saben qué datos almacenan, dónde los guardan ni cuál de ellos es prioritario proteger. Y lo más importante, una vez se detecten amenazas, debemos empezar a hablar acerca de ellas… en público.

Derribar el muro de silencio que rodea prácticamente todos los ciberataques es un paso esencial para apuntalar nuestra seguridad tecnológica común. Las empresas actuales conocen las repercusiones de que se haga público que han sido víctimas de un ataque informático. Más allá de los daños evidentes a la reputación, el coste de un ciberataque puede ser de cientos de millones de dólares derivados de las pérdidas directas, el recelo de los clientes y los litigios varios. Ello explica que las organizaciones hagan cuanto está en su mano por silenciar que han sido víctimas de un ciberataque, ya proceda éste de Crimen, S. A. o de una agencia de espionaje extranjera. Pero sucede que ese silencio palpita en el mismísimo corazón de los problemas de seguridad virtual que padecemos. Cuando una persona sobrevive a una agresión sexual, pero le abochorna o avergüenza demasiado como para denunciarla a la policía, el agresor no será detenido ni juzgado y seguirá disfrutando de libertad para agredir a otras víctimas. Pese a que un ciberataque es un delito de una índole muy distinta, sus víctimas también son reacias a denunciarlo públicamente. En consecuencia, estos incidentes no pueden agregarse y estudiarse, no se desarrollan defensas comunes y los artífices siguen campando a sus anchas para atacar otro día. Es imperioso rectificar esta situación. Guardar silencio acerca de estos riesgos no hace que desaparezcan; sencillamente los empeora y permite a los malhechores actuar con impunidad. En gran medida es como la decisión que hay que tomar para ir a Alcohólicos Anónimos, admitir que uno tiene un problema virtual es el primer paso y

el más importante para recuperarse.

Fomentar la resiliencia: automatizar las defensas y cambiar para bien

> Las nuevas tecnologías pueden emplearse con fines destructivos. La solución es desarrollar sistemas de reacción rápida ante los nuevos peligros, como un bioterrorista artífice de un nuevo virus biológico.
>
> RAY KURZWEIL

Los ciberataques ocurren y es imposible detenerlos todos. La cuestión de primer orden debe ser cómo podemos construir este mundo de rápida evolución tecnológica en el que vivimos de un modo mucho más resistente a estos ataques. No se trata de una pregunta con una respuesta fácil, dadas las complejidades de este sistema en expansión que están en juego. Un sistema resistente no falla de manera catastrófica, sino que se va degradando poco a poco con el tiempo hasta que se repara. Un sistema resistente continuará desempeñando sus funciones más importantes, aunque es posible que las actividades menos relevantes queden desactivadas o dejen de funcionar. La naturaleza ha creado estructuras excelentes de este tipo, tal como ejemplifica la lagartija. Cuando un depredador la ataca o agarra, la lagartija se desprende fácilmente de su cola, que vuelve a crecerle, lo cual le permite escapar y sobrevivir con las partes esenciales del cuerpo (el cerebro y los órganos reproductores). ¿Cuál es la cola de la lagartija de Internet o de tu red corporativa? Todavía no existe, y eso es algo que debemos solucionar.

Gran parte de nuestra infraestructura tecnológica está sujeta a puntos únicos de fallo, el más evidente de los cuales es la electricidad. Sin electricidad no hay Internet. O peor: sin electricidad no hay distribución del agua, producción de alimentos, transacciones financieras, comunicaciones ni transporte. Necesitamos aislar estas averías puntuales para que no se propaguen y necesitamos contar con fuentes energéticas alternativas que puedan adaptarse para prevenir estos tipos de «apagones», no sólo para la electricidad, claro está, sino para todas las herramientas tecnológicas que hacen posible la civilización actual.

Estos riesgos se extienden mucho más allá del tendido eléctrico e incluyen nuestros sistemas de *software* más habituales y la propia infraestructura de Internet. Muchas de las herramientas que hacen funcionar nuestro mundo tecnológico son, en esencia, como un monocultivo, es decir: funcionan con un *software* prácticamente idéntico que presenta las mismas vulnerabilidades. Los monocultivos informáticos, al igual que los agrícolas, están sujetos a fallos catastróficos (recuérdese la hambruna de la patata en Irlanda). En la actualidad, Microsoft Windows se ejecuta en más del 90

por ciento de los ordenadores de sobremesa de todo el mundo y, a comienzos de 2014, la asombrosa cifra del 95 por ciento de los cajeros automáticos de Estados Unidos seguían funcionando con Windows XP, un sistema operativo para el cual Microsoft ha dejado de crear actualizaciones de seguridad[1]. Los monocultivos tecnológicos son la savia de la vulnerabilidad informática masiva. Con sólo un *software* malicioso, los *hackers* pueden tener un profundo impacto mundial y conseguir que todas las copias del mismo proceso informático fallen de manera uniforme. Como hemos visto, los errores conocidos pueden campar a sus anchas durante años antes de que los fabricantes de *software* remienden estos agujeros. En el instante en que se detecta una brecha de seguridad en una versión de Windows 8 o Adobe PDF, debería dar comienzo el proceso de reparación mundial. Las empresas de *software* no deberían aguardar a que las personas corrijan manualmente sus sistemas aplicando el parche que crean (cosa que sabemos que la mayoría nunca hacemos). En su lugar, estos sistemas deberían ser autosanadores y buscar siempre las últimas versiones remendadas del *software* para garantizar que todas las puertas y ventanas conocidas de nuestra vida digital estén bien cerradas. Dicho de otro modo, no abordar las vulnerabilidades conocidas en decenas de millones de versiones del mismo programa del *software* en todo el mundo sería como mantener oculto el fallo mecánico que condujo al accidente de un 747, un fallo presente en todos los 747 operativos en el mundo, y dejar que esos aviones continuaran volando.

También debemos asegurarnos de que los ataques y las intromisiones individuales puedan aislarse para impedir su propagación. Pensemos en el ataque de 2013 contra el gigante comercial Target. Tal como se ha mencionado previamente, los piratas informáticos responsables de aquella intrusión lograron acceder a los terminales en los puntos de venta de Target tras vulnerar primero la red de un contratista responsable de mantener los sistemas de calefacción y aire acondicionado de los comercios. Si se hubiera detectado esa intrusión inicial, la pesadilla para la seguridad corporativa subsiguiente que vivió Target se podría haber evitado por completo. Necesitamos medios mejores y más resistentes de proteger nuestra información. Imaginemos una especie de *airbags* para nuestros datos. Cuando se produjera una brecha en los datos, estos *airbags* virtuales se activarían, encerrarían nuestras posesiones digitales y las protegerían de sufrir más daños.

Los presidentes ejecutivos y las juntas de dirección deberían preguntarse cuán resilientes son sus empresas. Por resiliencia se entiende ser capaz de permanecer operativo frente a un ataque sostenido por parte de oponentes sofisticados. Y aunque, como la lagartija, se pierda la cola, la empresa debe sobrevivir. Esto no sucederá por arte de magia, sino que requiere preparación mediante formación y entrenamiento. En concreto, la ciberresiliencia exige capacidad de adaptación para responder a un ataque y destreza para restablecer rápidamente las capacidades tecnológicas dañadas. Cómo curarse tras un ataque podría ser un aspecto decisivo a la hora de la supervivencia o la extinción de una empresa. Y el momento de responder a estas

preguntas no es durante una crisis, sino antes de que ésta se produzca.

Estos sistemas más resistentes que requerimos deben construirse desde el inicio. La seguridad no puede ser una consideración de última hora que se añade a la mezcla después de haber fabricado las máquinas. Es necesario que la ingeniería cree sistemas que fallen con suavidad, y no de manera cataclísmica. La computación segura y fiable deber ser la piedra angular de nuestro futuro tecnológico, para evitar que el conjunto del sistema se venga abajo. Y esto revestirá si cabe más importancia a medida que avancemos hacia la Internet de las Cosas y testimoniemos la llegada de tecnologías sumamente perturbadoras como la robótica, la inteligencia artificial y la nanotecnología. No podemos seguir ignorando las políticas públicas y las implicaciones legales, éticas y sociales de las herramientas tecnológicas que están apareciendo y evolucionan a un ritmo acelerado; somos moralmente responsables de nuestros inventos.

La historia contiene ejemplos paradigmáticos de una sociedad que ha recurrido a la experiencia y los conocimientos técnicos para anticiparse a los riesgos de las catástrofes antes de que sucedieran. Uno de estos casos fue la Conferencia de Asilomar sobre ADN Recombinantes de 1975, celebrada en Asilomar State Beach en Monterrey, California. El simposio reunió a 140 biólogos, abogados, eticistas y médicos para debatir los posibles riesgos biológicos de las tecnologías del ADN emergentes y trazó unas directrices de seguridad voluntarias. Tras la cita, los científicos acordaron poner fin a los experimentos que implicaran mezclar el ADN de distintos organismos, una investigación que por entonces tenía el potencial de provocar consecuencias radicales, poco entendibles e incluso desastrosas. Merece la pena recuperar las lecciones y los éxitos de Asilomar. Pese a que avanzamos a toda velocidad en los campos de la biología sintética, la inteligencia artificial, la robótica de enjambres y la nanotecnología, estamos dedicando unos recursos mínimos a entender los riesgos concomitantes de tecnologías que podrían replicarse fuera de nuestro control. Afortunadamente, en 2009 se celebró el mismo encuentro, en aquella ocasión en torno al futuro de la inteligencia artificial, en la misma playa de Monterrey y otras muchas congregaciones de este tipo han sido y siguen siendo cruciales para impulsar la resiliencia de un mundo edificado sobre tecnologías exponenciales.

Para dar un paso más allá, con el fin de apuntalar la seguridad de nuestra sociedad, hemos de adoptar otro cambio. Debemos ser capaces de responder a la mutación de los desafíos que afrontamos procedentes de una comunidad de piratas informáticos delincuentes completamente automatizada. Una y otra vez hemos visto a malhechores automatizar sus ataques. Precisamente esta capacidad ha derivado en un cambio de paradigma en la delincuencia, que ha pasado de ser un asunto de uno contra uno a ser un asunto de uno contra muchos. De ahí que sea posible que un grupo de la delincuencia organizada robe 1200 millones de contraseñas de cuentas mientras que otro lanza un destacable ataque DDoS de 70 gigabits por segundo que desactiva una docena de instituciones financieras. Las herramientas para cometer el

mal están mutando de manera exponencial, mientras que nuestros sistemas no se adaptan al ritmo necesario. Nuestras defensas no reaccionan lo bastante rápido para frenar los riesgos sistémicos globales que afrontamos, situación que debería preocupar profundamente a los gobiernos.

Reinventar el gobierno: innovación en frío

> No podemos resolver problemas usando el mismo tipo de pensamiento que usamos cuando los creamos.
>
> ALBERT EINSTEIN

En 2014, sólo el 13 por ciento de los estadounidenses aprobaban el trabajo que estaba haciendo el Congreso, una ligera mejora del perenne y bajísimo nueve por ciento registrado en noviembre de 2013[2]. La confianza en el gobierno de Estados Unidos es prácticamente inexistente, tanto por lo que concierne al dinero de la política, a las negaciones gubernamentales, el partidismo o la ausencia de una legislación significativa. Mientras que los cambios tecnológicos que nos rodean avanzan a un ritmo exponencial, el gobierno es claramente lineal en su velocidad de cambio. El desafío evidente ante tal asimetría es que nunca solucionaremos los problemas del siglo XXI con instituciones del siglo XIX. Necesitamos un gobierno con una capacidad de adaptación enorme, capaz de reaccionar diez veces más rápido, y eso sólo para mantenerse al día. Los secretarios de Gabinete y los magistrados del Tribunal Supremo que «no usan correo electrónico» no nos sirven.

La falta de innovación en el gobierno no sólo permea nuestras legislaturas, sino también los órganos de la seguridad nacional y el aparato de los cuerpos de seguridad. En respuesta a la creatividad (por diabólica que fuera) demostrada por los terroristas que llevaron a cabo los atentados del 11-S, el gobierno invirtió miles de millones de dólares y se le ocurrieron «innovaciones» como la Administración de Seguridad del Transporte. Y aunque cachear a niños de cuatro años y ancianitas en sillas de ruedas presenta un magnífico «panorama de seguridad», vamos a tener que jugar algo más fuerte si queremos tener alguna esperanza de evitar ataques terroristas en el futuro. Habida cuenta del ritmo de los cambios tecnológicos, las amenazas a la seguridad de mañana no se parecerán en nada a las actuales, uno de los motivos por los que el gobierno batalla poderosamente contra la ausencia de seguridad habitual en el mundo virtual.

Por supuesto no pretendo sugerir que no haya innovación en el gobierno. Fue el gobierno quien nos dio Internet y los viajes espaciales y quien sirvió de catalizador para descodificar finalmente el genoma humano. Es posible encontrar bolsas de innovación diseminadas por toda la estructura gubernamental, pero necesitamos que

estas gemas de la creatividad se repliquen y amolden de un modo que, hoy por hoy, sencillamente no está sucediendo. Uno de los modelos a seguir es Code for America, una organización sin ánimo de lucro que organiza a ciudadanos voluntarios con conocimientos de programación informática con el fin de hacer los servicios gubernamentales mucho más sencillos, efectivos y fáciles de utilizar. Otro ejemplo es el prestigioso GovLab de la Universidad de Nueva York, un laboratorio de innovación consagrado a utilizar la tecnología para rediseñar las capacidades de solucionar problemas de las instituciones gubernamentales. Respaldado tanto por la MacArthur Foundation como por la Knight Foundations, GovLab trabaja por el uso de tecnologías en red allende los paradigmas de control centralizados y de arriba abajo del pasado en pro de plataformas de autogobierno, innovación y participación ciudadana más proclives a la transformación.

No obstante, la idea fundamental es que, para que el gobierno siga ofreciendo una respuesta relevante a los desafíos más importantes y apremiantes que afrontamos hoy, necesitaremos inventar marcos completamente nuevos para la solución de problemas. En este aspecto, podemos inspirarnos en el Silicon Valley y empezar a concebir nuestros sistemas de gobernanza como los sistemas operativos de la sociedad. Si logramos cambiar la esencia del OS, todo lo demás cambiará con él. Las instituciones que hemos heredado luchan por sobrevivir, tanto la educativas como las de la salud y sanidad pública y los cuerpos de seguridad; la tecnología está dejando rezagada la capacidad de reacción del gobierno. Hasta el presente, en gran medida el planteamiento del gobierno con respecto a la seguridad tecnológica ha constituido en puro artificio y oportunidades perdidas. Tal como ha señalado Bryan Johnson, el empresario de Internet, necesitamos un nuevo sistema operativo para el mundo, un sistema basado en rudimentos y equiparable a los cambios exponenciales que nos rodean.

Afortunadamente, Johnson ha donado la generosa cifra de 100 millones de dólares de su riqueza personal a tal fin y ha creado el OS Fund para fomentar «descubrimientos de saltos cuánticos» a nivel de sistemas operativos con vistas a propiciar «un cambio real para la humanidad a escala mundial». Es evidente que las instituciones gubernamentales actuales no poseen el monopolio de las respuestas frente a muchos de los problemas que acechan a nuestro mundo, pero sí pueden desempeñar un papel relevante como conciliadoras, tendiendo puentes de diálogo entre los sectores público y privado como medio para hallar soluciones a algunos de los retos más notables.

Auténtica colaboración entre los sectores público y privado

Los esfuerzos gubernamentales para proteger a la población frente a las amenazas de la ciberdelincuencia y seguridad han demostrado ser totalmente inadecuados. ¿Debería sorprendernos? Las decenas de miles de ataques perpetrados con éxito contra Washington por parte de adversarios foráneos ponen en evidencia que el gobierno de Estados Unidos es incapaz siquiera de protegerse a sí mismo. La necesidad de que exista una colaboración más seria y profunda entre los sectores público y privado es manifiesta; sin ella, no haremos ningún progreso significativo por mejorar la situación general de nuestra seguridad. Esta necesidad es especialmente imperiosa en lo tocante a la protección de las infraestructuras esenciales del país, el 85 por ciento de las cuales están en manos del sector privado[3]. En tanto que nación y en tanto que personas, necesitamos que el gobierno y el sector industrial cooperen para proteger la maquinaria del mundo moderno. La pregunta es cómo.

Conscientes de la necesidad de que exista una colaboración entre los sectores público y privado, instituciones tan diversas como el FBI, la Unión Europea y el Foro Económico Mundial han establecido programas para impulsar una mayor cooperación entre los responsables de gestionar las infraestructuras básicas del mundo. Iniciativas adicionales, como los Centros de Análisis y Compartición de Información, contribuyen a que sectores específicos como los servicios financieros, el sector de la energía y el sector de las comunicaciones colaboren y respondan mejor a los ciberataques. El Forum of Incident Response and Security Teams también ha tenido un papel influyente en la mejora de la coordinación y la respuesta entre pares de confianza tanto en los CERT (Computer Emergency Response Teams o Equipos de Respuesta ante Emergencias Informáticas) tanto gubernamentales como del sector privado. Los conatos de colaboración entre el sector público y privado han demostrado ser útiles, sin lugar a dudas, pero también han recibido críticas puntuales por la falta de definición de cometidos y por los escasos objetivos específicamente articulados más allá de «compartir información».

Es preciso superar problemas reales para que los regímenes de compartición de información entre el sector público y privado alcancen todo su potencial. El sector privado en general acusa una falta de confianza en que el gobierno mantenga la confidencialidad, sobre todo a la hora de revelar datos de ciberamenazas a la competencia, por no hablar ya de protegerse del riesgo antimonopolio. También el gobierno afronta desafíos: debe idear una manera de compartir sus conocimientos acerca de ciberriesgos concretos, muchos de los cuales son información clasificada, con empresas y personal técnico que carecen de la autorización necesaria para ver material clasificado. Un informe de 2010 de la Oficina Gubernamental de Contabilidad de Estados Unidos determinó que menos de un tercio de la empresa que participa en colaboraciones en materia de ciberseguridad con el gobierno tenía la sensación de estar recibiendo información acerca de las ciberamenazas que les permitiera actuar[4].

La exigencia que plantean los peligros tecnológicos que tenemos por delante implica que debemos superar estas tribulaciones con mucha mayor urgencia con el fin de impulsar auténticas colaboraciones entre el sector gubernamental y el sector privado.

Un aspecto particularmente positivo en este sentido ha sido la Red de Innovación en Seguridad (SINET por sus siglas en inglés, de *Security Innovation Network*), cuyo cometido es fomentar la innovación en el campo de la ciberseguridad tendiendo puentes entre los sectores privado y público. La SINET se fundó en San Francisco y sirve de conector (una suerte de intérprete entre el Silicon Valley y quienes habitan en el interior de Beltway). Al aunar a agentes destacados de ambos mundos, la SINET ha contribuido a impulsar el espíritu emprendedor y la innovación entre todas las partes que trabajan en el ecosistema de la ciberseguridad para concentrarlas en la misión que les ocupa. Más allá de las personas que en el seno del gobierno y el sector industrial se encargan a jornada completa de combatir las ciberamenazas, puede incorporarse otra fuerza espectacular para bregar con los desafíos que afrontamos: un público general instruido.

Nosotros, el pueblo

No es fe en la tecnología. Es fe en las personas.

STEVE JOBS

Contemplar el amplio alcance y la magnitud de las actividades maliciosas perpetradas por la delincuencia organizada, el terrorismo, los piratas informáticos y gobiernos corruptos es suficiente para que cualquiera se sienta desalentado, asustado e incluso deprimido. No obstante, si hay algo que me solaza tras cerca de dos décadas de trabajar en el ámbito de la seguridad mundial es que en este mundo el número de buenas personas supera con creces al de malas personas. Y eso supone una inmensa ventaja, pese a que aún no la hemos aprovechado plenamente en nuestro beneficio. Crimen, S. A. tiene amplios conocimientos acerca de los proveimientos participativos y es capaz de movilizar a muchedumbres de miles de personas, tal como vimos con el ciberataque a los cajeros automáticos de 2013, en el que los ladrones realizaron treinta y seis mil operaciones en persona en diez horas y en veintisiete países y se embolsaron la asombrosa cifra de 45 millones de dólares. Un episodio fascinante por su velocidad, proeza, innovación e impacto. En cambio, ¿dónde está la seguridad pública equivalente a un ataque de esta índole? Todavía no existe y eso es algo que tiene que cambiar si queremos reforzar nuestras autodefensas y la confianza en nosotros mismos en el amanecer de esta nueva era digital.

Por doloroso que sea, me ha quedado perfectamente claro que nuestras autoridades están perdiendo la ventaja tecnológica frente a la delincuencia. Los cuerpos de seguridad, superados de trabajo y socavados por los recortes presupuestarios, están siendo asaltados y batallan por mantenerse actualizados. Pero aún hay más: la policía es un sistema cerrado, de ámbito nacional, mientras que la amenaza es internacional. Los paradigmas de seguridad actuales, tanto armas como guardia fronteriza y vallas de gran altura, están absolutamente desfasados. No son capaces de frenar el paso de bits y *bytes*, que recorren el mundo a la velocidad de la luz. Para superar estos vacíos palmarios en las actuales instituciones de seguridad pública, debemos hallar modos más radicales y novedosos de abordar el problema, modos que incorporen una forma de lucha contra la delincuencia más radical y participativa. ¿Dónde están los programas de vigilancia del vecindario y de patrullas comunitarias? En lugar de contar con un reducido equipo de élite de agentes altamente preparados para que nos protejan, nos iría mucho mejor formar a la ciudadanía para que combata estos problemas en tanto que colectivo mediante el proveimiento participativo. Para derrotar a Crimen, S. A. en su juego, no sólo hemos de perfeccionar nuestra capacidad de adaptarnos, sino que además hemos de crecer y mejorar.

La idea de que los cuerpos de seguridad apliquen los métodos del proveimiento participativo no es nueva. En 1865, cuando John Wilkes Booth asesinó al presidente Lincoln, se convirtió en el primer felón huido cuya fotografía apareció en un cartel de «Se busca». Hoy, 150 años después del asesinato del decimosexto presidente de Estados Unidos, la aplicación de proveimientos participativos en los cuerpos de seguridad por parte del gobierno no ha cambiado ni un ápice. Los policías distribuyen fotografías a las cadenas de noticias locales, cuyos presentadores advierten que la persona buscada «va armada y es peligrosa» y añaden: «Se ruega a los testigos oculares que se pongan en contacto con la policía». Parece una broma pesada. Sin duda en 2015 podemos hacer algo mejor para impulsar la participación pública, aparte del típico «si ve tal, haga cual».

Nosotros, el pueblo, al igual que Crimen, S. A., podemos aprovechar la munificencia que proporciona la tecnología para protegernos y defendernos. Clay Shirky utiliza el término «excedente cognitivo» para describir la «capacidad de la población mundial de ofrecerse voluntaria, hacer aportaciones y colaborar en proyectos a gran escala, incluso mundiales». Ha llegado el momento de que nosotros, el pueblo, empecemos a utilizar nuestro excedente cognitivo para proteger y defender nuestro futuro. La guerra del código abierto y la delincuencia por proveimiento participativo deben frenarse con una seguridad de código abierto y una seguridad pública mediante proveimiento participativo. Por suerte, hay algunos puntos brillantes en los que este nuevo paradigma de la seguridad pública empieza a resplandecer. Organizaciones como Crisis Commons y Ushahidi están reinventando la provisión de ayuda humanitaria tras un desastre y están salvando vidas mediante la

coordinación de la respuesta ciudadana en casos de emergencia pública, inclusive durante el terremoto de Haití y el ataque terrorista en el centro comercial Westgate Mall de Nairobi. Ciudadanos de México, un país atormentado por los cincuenta mil homicidios relacionados con el narcotráfico entre 2006 y 2012, utilizan herramientas como Google Maps para informar mediante proveimiento participativo acerca de los cárteles, sus actividades y su paradero[5]. Y en la Europa del Este, el Organized Crime and Corruption Reporting Project[*], en el que participan tanto periodistas como ciudadanos, colabora mediante proveimiento participativo en sofisticadas investigaciones multinacionales acerca del paradero de dictadores, funcionarios corruptos, terroristas y grupos de delincuencia organizada, así como del blanqueo de sus ganancias ilícitas obtenidas en todo el mundo. Y ya que hablamos de corrupción pública, en 2009, editores del diario británico *The Guardian* crearon un *software* que permitía a los ciudadanos «investigar en común» más de 455 000 páginas de datos que habían obtenido con el fin de identificar transgresiones flagrantes en los gastos de los parlamentarios del Reino Unido. Más de veinticinco mil ciudadanos voluntarios participaron en la investigación digital, y los resultados fueron verdaderamente asombrosos. Se revisaron más de 170 000 documentos en las primeras ochenta horas y el descubrimiento por parte del público de miles de flagrantes apropiaciones indebidas de fondos públicos obligó a la destitución y renuncia de numerosos parlamentarios, ministros e incluso del portavoz de la Cámara de los Comunes, un resultado auténticamente devastador acaecido por última vez en 1695[6].

En todos estos casos, la ciudadanía pudo hacer algo más que simplemente denunciar delitos a las autoridades. Se le permitió reunir pruebas canalizando tiempo y energía para descifrar datos con el fin de propiciar resultados mucho más rápido de lo que ninguna fuerza policial u organización gubernamental habría sido capaz de hacer por sí sola. El planteamiento de la seguridad pública como un proveimiento participativo arroja claros resultados y debe convertirse en un elemento integral de nuestra estrategia global de seguridad en un mundo que cambia de manera exponencial y en el que, sobre todo, escasea el personal dedicado a la ciberseguridad a jornada completa. La Rand Corporation ha señalado que la escasez nacional de profesionales técnicos en materia de seguridad en el seno del gobierno federal es tan crítica que pone en riesgo la seguridad del país[7]. Tal revelación halló eco en el informe de Cisco *2014 Annual Security Report*, que calculaba que faltaban más de un millón de profesionales de la ciberseguridad en todo el mundo y que se preveía que dicha cifra aumentase a dos millones en 2017[8]. Necesitamos desesperadamente más implicación del público para proteger nuestro futuro tecnológico e incluso los canales del funcionariado han comenzado a aceptarlo.

En 2012, el abogado estrella del FBI en temas de Internet, Steven Chabinsky, tildó los esfuerzos gubernamentales por luchar contra la ciberdelincuencia de «enfoque fallido» y añadió que se requerirían esfuerzos mucho más notables por parte de la población para combatir las ciberamenazas[9]. Ese trabajo está empezando

a fraguar. En un caso, un profesor de la Universidad de Alabama y los alumnos de su clase de Derecho Penal colaboraron con el FBI en la desarticulación de un anillo de ciberdelincuencia de 70 millones de dólares propiedad de Crimen, S. A. en Ucrania y Rusia. La «investigación participativa» emprendida por los estudiantes identificó con éxito a numerosos sospechosos en Estados Unidos que habían utilizado el troyano de la banca Zeus para robar millones, individuos que finalmente fueron arrestados por el FBI como resultado del trabajo de los alumnos[10]. Ahora bien, para poder tener un éxito duradero y significativo, tales esfuerzos de proveimiento participativo no pueden ser meramente *ad hoc*, sino que deben formalizarse sistemáticamente para poderse amoldar a la envergadura de la amenaza. En 2011, la policía del Reino Unido dio un paso en esas dirección al crear una estructura nacional de agentes especiales voluntarios con conocimientos relevantes para colaborar en la lucha contra la ciberdelincuencia[11].

En Estados Unidos y en el resto del mundo, deberíamos inspirarnos en estos éxitos y llevarlos aún más allá. Ya contamos con agentes de policía auxiliares y en la reserva. En el ejército hay soldados en la reserva, soldados de las fuerzas aéreas y de la marina y soldados que compaginan la vida civil y la vida militar. En el bando de la sociedad civil, tenemos a Peace Corps y AmeriCorps. Ahora necesitamos un Cuerpo de Ciberdefensa Civil Nacional. Una organización de estas características recordaría a otros esfuerzos de defensa acometidos por la sociedad civil en la historia de nuestro país que se remontan a la Primera Guerra Mundial. Podrían reclutarse expertos de todos los ámbitos de la sociedad para que protegieran frente ataques las infraestructuras de la información esenciales y nuestra nación de las crecientes amenazas tecnológicas que se ciernen sobre nosotros. Los miembros de este organismo se seleccionarían con esmero y se someterían a extensos programas de formación, además de revisarse su trasfondo, y trabarían en el seno de marcos legales y operativos claramente definidos. El tiempo es esencial para establecer y construir una fuerza participativa de esta índole: hemos de hacerlo ahora, antes de que se produzca la cibercrisis. Multitud de organizaciones profesionales del sector privado podrían ser sumamente valiosas para ayudar a impulsar estos esfuerzos, como el International Information Systems Security Certification Consortium o $(ISC)^2$, una organización sin ánimo de lucro integrada por más de 100 000 profesionales de la ciberseguridad certificados capaces de tener un impacto positivo en cualquier programa de su elección.

Crimen, S. A. está ocupada reclutando compinches para sus fechorías. ¿No deberíamos estar haciendo lo mismo? Personas de todos los colores y todos los trasfondos pueden ayudar en esta empresa: jóvenes, ancianos e incluso algunos piratas informáticos que cuenten con las habilidades para marcar la diferencia, en el caso de que prefieran destinar su talento en beneficio público. Tal como nos recuerda el cofundador de Apple, Steve Wozniak, «Es bueno que haya gente que rompe las reglas». Debemos crear oportunidades, sobre todo para los jóvenes, con el fin de que

canalicen su considerable talento y energía para bien si no queremos que Crimen, S. A. los reclute para hacer el mal. La esencia exponencial de la tecnología y la respuesta lineal del gobierno implican que precisaremos más manos en la baraja para construir una sociedad segura y estable que no se destruya a sí misma. Nuestra seguridad pública es demasiado importante para que la releguemos únicamente a manos de los profesionales. En el mundo actual, que avanza exponencialmente, en la lucha entre el bien y el mal, la victoria caerán en manos del grupo que demuestre ser capaz de movilizar a la multitud más numerosas. Ha llegado el momento de tomar la delantera y volver este sistema a nuestro favor para asegurarnos de que las herramientas tecnológicas se empleen en beneficio de toda la humanidad.

El juego del sistema

> Todo diseñador de juegos debería crear un juego que cambiara el mundo de manera explícita. Los abogados trabajan sin cobrar, ¿por qué no podemos hacerlo nosotros también?
>
> JANE MCGONIGAL

De acuerdo con la diseñadora de juegos e investigadora estadounidense Jane McGonigal, en la actualidad hay más de 500 millones de personas en el mundo que juegan a juegos de ordenador y videojuegos al menos una hora al día, y más de 183 millones sólo en Estados Unidos. Eso representa tres mil millones de horas a la semana jugando a videojuegos en tanto que planeta[12]. ¿Qué sucedería si esos esfuerzos se canalizaran a hacer el bien público? Imagina la fuerza y el tremendo potencial que podría desatarse. Hacerlo permitiría encauzar la sabiduría de las multitudes para afrontar algunos de los mayores desafíos que apremian al mundo. Para poner a prueba esta teoría, en 2009 DARPA creó su Network Challenge (también conocido como Red Balloon Challenge), consistente en ocultar diez grandes globos de helio rojos al aire libre en todo Estados Unidos, en ciudades desde Miami hasta Portland, y ofrecer un premio de 40 000 dólares al primer equipo que localizara todos los globos. DARPA concibió este concurso con el fin de investigar el papel que podían desempeñar Internet y las redes sociales en la comunicación en tiempo real y la colaboración de área extensa con vistas a resolver problemas con un tiempo limitado, como la ayuda humanitaria tras un desastre en tiempos de crisis. Sorprendentemente, un equipo del MIT localizó los diez globos en los puntos más lejanos del país en sólo nueve horas, propagando mediante proveimiento participativo la labor por las redes sociales a cuatro mil cuatrocientos voluntarios.

Así que resulta que jugar a juegos no siempre es una pérdida de tiempo, sino que puede ser una actividad muy productiva. La ludificación es un nuevo campo de

estudio que permite utilizar el pensamiento y la mecánica de los juegos en contextos no lúdicos con el fin de motivar e involucrar a los jugadores en la resolución de problemas del mundo real. Un ejemplo de ello se ha dado en la salud pública, concretamente en el diagnóstico y tratamiento de la malaria. En todo el mundo se dan más de 600 000 casos de malaria al día y muere un niño cada minuto. La enfermedad se contagia por picaduras de mosquito que transfieren parásitos al cuerpo humano e infectan los glóbulos rojos. Diagnosticar la malaria consume mucho tiempo, pues el especialista puede pasar hasta treinta minutos buscando parásitos en la sangre bajo el microscopio, lo cual hace que muchas personas no se diagnostiquen bien y mueran. MalariaSpot es un juego que subsana este problema presentando a los jugadores imágenes virtuales de muestras de sangre de pacientes reales y desafiándolos a etiquetar tantos parásitos como encuentren en sólo un minuto. Los resultados fueron impresionantes: en sólo un mes, jugadores anónimos de noventa y cinco países jugaron doce mil partidas. Tras recibir un breve explicación y formación en línea acerca del aspecto de los parásitos, los jugadores de MalariaSpot han identificado correctamente más de 700 000 diagnósticos parasitarios. Puesto que la misma imagen se muestra a múltiples jugadores, éstos, que no son expertos médicos, han alcanzado una tasa de precisión superior al 99 por ciento, un «cambio de juego» en el mundo del diagnóstico y tratamiento de la malaria[13]. En otro caso, un juego titulado Foldit permite a los miembros del público sin formación especializada en biología molecular solucionar rompecabezas científicos utilizando sus conocimientos de orientación espacial en 3D para manipular y plegar moléculas de proteínas como medio de estudiar y tratar enfermedades. En un caso memorable, los jugadores de Foldit identificaron correctamente la estructura de una enzima crucial para la reproducción del VIH en apenas unos días, un descubrimiento que había eludido a los equipos de investigación del sida en todo el mundo, quienes habían intentado activamente resolver el problema durante más de una década[14].

Los juegos de proveimiento participativo como MalariaSpot y Foldit deberían proporcionar una inspiración trascendental e importantes lecciones extrapolables al problema de la inseguridad tecnológica. ¿Qué rompecabezas entretenidos podríamos crear para conseguir que la población, en concreto la juventud, canalice su pasión por los juegos para mejorar la ciberseguridad? Imagina las posibilidades. En lugar de presentar muestras de sangre para buscar parásitos de la malaria, podríamos presentar correos electrónicos de *phishing* en tiempo real y solicitar al público que identifique correctamente las solicitudes maliciosas de datos bancarios, y recompensar con puntos y premios a los mejores jugadores. La ludificación del *software* de seguridad podría ayudar a las empresas de tecnología a erradicar el inconveniente de la mentalidad «Envíalos y ya está» al conseguir que decenas de miles de jugadores de todo el mundo fueran a la «caza de bugs» y detectaran los fallos de sus productos de *software* y *hardware*, fallos que, de otro modo, aprovecharían los piratas informáticos de Crimen, S. A. en detrimento del público. Esta idea ya está siendo objeto de estudio

por parte de DARPA, así como de diversas empresas noveles, como Topcoder y Bugcrowd. Estas mismas técnicas podrían aplicarse también a los sistemas de las infraestructuras básicas de Estados Unidos. Podría presentarse a los jugadores datos anónimos en un juego animado al estilo de SimCit y permitirles que hallaran vulnerabilidades a la seguridad en todo tipo de cosas, desde tendidos eléctricos virtuales hasta redes de transporte. Al final, cada jugador tendría el potencial de hacer un gran descubrimiento para la ciberseguridad y hacerlo sin más motivación que jugar y disfrutar. A otros los motivaría su capacidad de resolver problemas del mundo real y ayudar a sus iguales. Y para aquéllos a quienes no seduce ninguna de ambas ideas, siempre habrá dinero contante y sonante.

El ojo en el premio: concursos para mejorar la seguridad mundial

> El día antes de que algo se vuelva un gran avance se considera una idea chiflada.
>
> PETER DIAMANDIS

Los premios ayudan a concentrarse. Si no, pregúntaselo a las muchedumbres que se presentan para tener la posibilidad de llevarse el gordo de la lotería. Pero, además, los premios pueden ser la chispa que engendre una solución revolucionaria para un problema intratable. Así se demostró cuando el Parlamento británico estableció el Premio Longitud en 1714, en un intento por ayudar a la navegación marítima y garantizar la «seguridad y la velocidad de los viajes, la conservación de los buques y las vidas de los hombres». Pese a que la latitud (posicionamiento en el eje norte-sur) era fácil de calcular usando la posición del sol, hasta principios del siglo XVIII los marineros no tuvieron modo de calcular su posición longitudinalmente de este a oeste. Mediante una ley parlamentaria, el gobierno británico ofreció 20 000 libras esterlinas (más de un millón de libras actuales) por una solución que pudiera determinar la longitud en menos de medio grado. El incentivo del premio inspiró a John Harrison, un relojero de clase obrera autodidacta, a inventar el cronómetro marino, un dispositivo parecido a un reloj que resolvió aquel problema. Doscientos años más tarde se lanzó otro premio de incentivo, en esta ocasión para estimular el progreso en el campo incipiente de la aviación.

Charles Lindbergh se convirtió en el primer hombre que sobrevoló el Atlántico, no sólo movido por su espíritu aventurero, sino porque un magnate hotelero apenas recordado llamado Raymond Orteig ofreció 25 000 dólares de su propio bolsillo en 1919 como premio «al primer aviador de cualquier país aliado que atravesara el

Atlántico sin repostar, de París a Nueva York y de Nueva York a París». Orteig ofreció la recompensa para impulsar una estimulante tecnología nueva de aquellos tiempos: la máquina voladora. Tal empresa no estuvo financiada por ningún gobierno y no generaría beneficios de inmediato, pero ello no detuvo a nueve equipos distintos de gastarse en torno a 400 000 dólares para hacerse con el premio de 25 000. Aquella recompensa fue la leña que avivó el fuego, la chispa que desató la innovación, resolvió el enigma y ayudó a crear la industria de la aviación actual. En 1996, el físico, entusiasta del espacio y empresario empedernido Peter Diamandis tomó el testigo a Orteig y fundó la XPRIZE Foundation, una organización sin ánimo de lucro que diseña y dirige concursos públicos destinados a alentar el progreso tecnológico para la mejora de la humanidad. Quizá sea hora de que convoque un concurso en torno al tema de la ciberseguridad.

De acuerdo con Diamandis, «Un XPRIZE es un concurso con premio influyente e incentivado que amplía los límites de las posibilidades para hacer un mundo mejor. Seduce la imaginación del mundo e inspira a otros a alcanzar objetivos similares, espoleando con ello la innovación y acelerando el ritmo de los cambios positivos». El primer concurso de la historia anunciado por Diamandis fue el Ansari XPRIZE, con un premio de diez millones de dólares, que desafiaba a los equipos a lanzar una nave espacial tripulada más allá de la línea de Kármán (100 km de altitud) y regresar sanos y salvos a la Tierra. Por si ello no fuera suficiente, las reglas también establecían que la nave espacial debía ser capaz de acomodar el peso de dos adultos más y realizar un segundo lanzamiento en un espacio de dos semanas. Sin financiación gubernamental, veintiséis equipos gastaron más de 100 millones de dólares intentando alcanzar aquel noble objetivo y, en otoño de 2004, el equipo de Mojave Aerospace Ventures logró su cometido y allanó el camino para el turismo espacial y otros vuelos espaciales comerciales. Los premios de incentivo son osados y audaces y captan la atención del mundo… justamente el tipo de pensamiento que necesitamos para dar un gran salto adelante y protegernos de los profundos riesgos tecnológicos que afrontamos.

Un XPRIZE de la ciberseguridad podría servir como motor de innovación, un estímulo espectacular para impulsar un cambio exponencial para bien y dirigir la inseguridad tecnológica del mundo en el beneficio general de la humanidad. Definiendo claramente los problemas de ciberseguridad a los que nos enfrentamos, el XPRIZE podría incentivar a equipos de todo el mundo a hallar las soluciones más eficaces de un modo que bien podría evitar crisis, facultar a las personas, generar nuevas tecnologías e incluso propiciar la aparición de nuevas industrias. Un XPRIZE a la ciberseguridad nos podría ayudar a superar uno de los desafíos posiblemente más grandes que afrontamos con relación a los riesgos que plantean las tecnologías exponenciales: la convicción en que estos problemas son intratables e irresolubles y no existe un camino claro que conduzca a una solución. Mentira. Hemos vivido tiempos arduos en el pasado y, como especie, hemos conseguido repetidamente cosas que el día antes se consideraban una chifladura. Los premios de incentivo alientan la

esperanza mediante la concepción de un mundo mejor y quienes los ganan dan fe de que algunos de los problemas que parecían imposibles pueden resolverse. Una persona sola o un pequeño equipo pueden suponer una gran diferencia, tal como han demostrado Lindbergh, Harrison e incontables otros en el pasado. Y lo más importante, un premio XPRIZE a la ciberseguridad podría ser sólo el principio para registrar grandes progresos en la seguridad mundial. Otras amenazas emergentes, como el bioterrorismo, la inteligencia artificial desbocada, los sistemas de armas autónomas y la nanotecnología también merecen la convocatoria de concursos de incentivo, sobre todo dado el riesgo potencialmente existencial que podrían plantear al mundo.

De la misma manera que el filántropo Raymond Orteig incentivó la aviación civil y Anousheh y Amir Ansari estimularon la industria espacial comercial, los filántropos de la actualidad también pueden marcar la diferencia en la seguridad de las tecnologías. Piénsese, si no, en los asombrosos hitos que ha conseguido la Bill and Melinda Gates Foundation en la lucha contra el VIH, la erradicación de la polio y el fomento de la educación, distribuyendo la asombrosa cifra de 26 000 millones de dólares de la riquezas del señor Gates desde su creación. Y no están solos, sino que existe toda una nueva raza de «tecnofilántropos» en el mundo, comprometidos a utilizar sus riquezas para generar un mundo mejor. El primer presidente de eBay, Jeff Skoll, ha emprendido una cruzada incansable contra las pandemias y la proliferación nuclear, dotando a su fundación con cerca de mil millones de dólares de su capital privado. Elon Musk, Pierre Omidyar, Paul Allen, Steve Case, Larry Ellison, Mo Ibrahim, *sir* Richard Branson y Michael Bloomberg tuvieron la increíble generosidad de rubricar la campaña «The Giving Pledge[*]» y con ello se han comprometido a donar la mayor parte de su riqueza con fines filantrópicos. A estas personas las mueven pasiones personales que apoyan de manera activa con su riqueza, pasiones que abarcan desde el buen gobierno hasta el desarrollo infantil. Dado que la mayoría de las personas citadas anteriormente ganaron toda o parte de su riqueza trabajando en el sector de la tecnología, financiar un XPRIZE centrado en este tema representaría dar un paso de gigante en la lucha contra las amenazas tecnológicas emergentes que tenemos delante y, con su experiencia en la materia, podrían marcar una diferencia inmensa. Felizmente, la XPRIZE Foundation se encuentra en las fases iniciales de explorar un XPRIZE a la ciberseguridad, con el apoyo de Deloitte Consulting. Incluso una bolsa de 20 millones (un mero 0,01 por ciento de los ingresos anuales generados por la industria del *software*, que mueve 150 000 millones de dólares) representaría un cambio enorme en el camino para proporcionar el *software* más estable y seguro requerido para proteger nuestro futuro tecnológico. Aún así, puede hacerse algo todavía más grande y atrevido, y de la misma escala y alcance que los desafíos tecnológicos apremiantes que afrontamos.

Pongámonos serios: un Proyecto Manhattan[*] para el mundo virtual

> Durante mi participación en el Proyecto Manhattan y la subsiguiente investigación en Los Álamos, que abarcó un período de quince años, trabajé en la compañía de la que tal vez fuera la mayor concentración de talento científico que el mundo haya conocido nunca.
>
> FREDERICK REINES

Cuando en 1939 se descubrió que los físicos alemanes habían aprendido a dividir el átomo de uranio, no tardó en diseminarse entre la comunidad científica estadounidense el temor a que los nazis pronto tuvieran la capacidad de crear una bomba capaz de una destrucción inimaginable. Albert Einstein y Enrico Fermi acordaron que había que exponer la situación al presidente estadounidense Franklin Delano Roosevelt. Poco después se lanzó el Proyecto Manhattan, un esfuerzo secreto épico de los Aliados durante la Segunda Guerra Mundial para crear un arma nuclear. Las instalaciones se ubicaban en Los Álamos, Nuevo México, y se designó a Robert Oppenheimer como supervisor del proyecto. Entre 1942 y 1946, el Proyecto Manhattan empleó de manera clandestina a más de 120 000 norteamericanos que hacían turnos las veinticuatro horas del día a todo lo ancho y largo del país, por un coste de 2000 millones de dólares. Quienes trabajaban en el Proyecto Manhattan se tomaban muy en serio la amenaza que afrontaban. Nosotros no lo hacemos.

Si bien ninguna persona en su sano juicio equipararía los riesgos del catastrófico impacto de una guerra nuclear con el robo de 100 millones de tarjetas de crédito, algunos de los descubrimientos científicos en curso hoy en día, incluidas la inteligencia artificial, la nanotecnología y la biología sintética, sí tienen el potencial de suponer una amenaza tremenda para la vida en este planeta, tal como han advertido Stephen Hawking y Elon Musk, entre otros. Más allá de estas amenazas existenciales en potencia, lo primero que debemos hacer es reconocer que los cimientos de la sociedad tecnológica moderna, encarnados en las infraestructuras de información esenciales mundiales, son débiles y podrían desmoronarse debido a su arquitectura envejecida y decadente, a complejidades abrumadoras del sistema o como consecuencia de un ataque directo de malhechores.

Aunque aún no hemos padecido ese ciberataque calamitoso que redefinirá el sector y acerca del cual nos han prevenido tanto, ¿por qué tenemos que esperar a padecerlo para prepararnos? Por doquier hallamos pruebas de peligros tecnológicos. A diario, ciberataques perturban el sistema financiero, ladrones roban propiedad intelectual valorada en miles de millones de dólares, países extranjeros hurtan los planes de armamento militar estadounidenses y piratas informáticos comparten en Internet consejos sobre cómo apoderarse de los sistemas de control industrial con los que funciona prácticamente todo, desde centrales nucleares hasta instalaciones de

tratamiento de agua y residuos. Parafraseando al célebre estadístico y editor del blog *FiveThirtyEight*, Nate Silver, el enfoque abúlico actual de la ciberseguridad y las hondas vulnerabilidades tecnológicas que tenemos delante han sido hasta la fecha como aplicarnos crema solar y afirmar que nos protege de una fusión nuclear, absolutamente inadecuado para la magnitud del problema. Es hora de replantearnos fríamente y en serio la situación actual. Es hora de crear un Proyecto Manhattan para la ciberseguridad.

No soy el primero en sugerir que se acometa un proyecto de tales características; muchos otros lo han hecho hasta la fecha, sobre todo en la estela de los atentados terroristas del 11-S. A la sazón, una coalición de científicos prominentes escribió una carta al presidente George W. Bush en la que advertían: «Las infraestructuras esenciales de Estados Unidos, incluyendo el tendido eléctrico, las finanzas, las telecomunicaciones, la sanidad, el transporte, el agua, la defensa e Internet, son altamente vulnerables a ciberataques. Se requiere emprender acciones mitigadoras ágiles y resueltas para evitar una catástrofe nacional». Entre los signatarios de aquella carta figuraban académicos, grupos de expertos, empresas de tecnología y organismos gubernamentales, incluidos los exdirectores de DARPA, la CIA, el Defense Science Board, Xerox PARC, diversos laboratorios estadounidenses y universidades de la Ivy League[*]. Estos pensadores sesudos, con poca tendencia a la hipérbole o la exageración, advertían que el grave riesgo de un ciberataque era un peligro real y presente y solicitaban al presidente que adoptara medidas inmediatas, como la creación de un proyecto de ciberdefensa a imagen y semejanza del Proyecto Manhattan. Tal llamamiento a la acción se produjo en 2002. Por desgracia, apenas ha cambiado nada desde entonces con relación a la situación de la ciberinseguridad mundial; a lo sumo, la situación ha empeorado. Por descontado que ha habido esfuerzos nominales y se han recolocado algunas sillas en la cubierta proverbial del *Titanic*, pero lo cierto es que no ha habido ningún progreso sustancial. ¿Cuál es la estrategia global de Estados Unidos para protegerse de las amenazas tecnológicas crecientes que afrontamos? Sencillamente, no tenemos ninguna estrategia, un grave problema que quizá algún día tengamos que lamentar.

Un verdadero Proyecto Manhattan para el mundo virtual aunaría a algunas de las mentes más preclaras de nuestro tiempo, procedentes tanto del ámbito gubernamental como del académico, del sector privado y de la sociedad civil. En el papel de coordinador e inversor, el gobierno reuniría a los científicos informáticos, emprendedores, autoridades en datos masivos, investigadores científicos, inversores en capital riesgo, abogados, expertos en políticas públicas, agentes de los cuerpos de seguridad y funcionarios de salud pública, así como al personal militar y de inteligencia más brillante. Su cometido sería crear una auténtica ciberdefensa nacional capaz de detectar y reaccionar a amenazas contra las infraestructuras esenciales del país en tiempo real. Este Proyecto Manhattan contribuiría a generar las herramientas relacionadas que necesitamos para protegernos, incluidos sistemas

operativos más robustos, seguros y garantes de la privacidad. A través de la investigación, también diseñaría y produciría *software* y *hardware* con capacidad autosanadora e inmensamente más resistente a los ataques y resiliente a los fallos que cualquiera disponible en el presente. Un proyecto tal, de trascendencia nacional y planetaria, partiría de un buen planteamiento, tendría un amplio alcance y estaría dotado de recursos y del presupuesto necesario para convertirlo en un éxito.

Y lo más importante, debería estar imbuido de una sensación de urgencia proporcional al Proyecto Manhattan original, algo que hasta ahora ha brillado por su ausencia en nuestros intentos poco entusiastas, tanto pretéritos como actuales, de lidiar con la creciente falta de seguridad en Internet.

Por desmoralizante que pueda parecer esta tarea, tengo una buena noticia que darte. Es posible hacerlo. Podemos ganar esta batalla. Nuestra condición de personas nos dota de lo necesario para influir profundamente en el avance de la seguridad común. Se precisará visión, foco y liderazgo. Y, aunque en ocasiones pueda parecer inútil, dejemos que nos aliente el presidente John F. Kennedy, quien, en un discurso pronunciado en la Rice University en septiembre de 1962, convenció al pueblo de Estados Unidos de financiar la NASA y, en menos de una década, el hombre fue a la Luna y regresó a la Tierra sano y salvo. En su elocuente y enardecedor discurso ante treinta y cinco mil espectadores, el presidente Kennedy ensalzó la importancia de los viajes espaciales como parte integral de la seguridad mundial, afirmando:

> El hombre, en su búsqueda del conocimiento y el progreso, está decidido y no puede ser disuadido […] Hemos prometido que no veremos un espacio repleto de armas de destrucción masiva, sino de instrumentos de conocimiento y comprensión. […] Zarpamos en este nuevo mar porque hay nuevos conocimientos que adquirir, nuevos derechos que ganar, los cuales se deben adquirir y usar para el progreso de todas las personas. Porque la ciencia espacial, al igual que la ciencia nuclear y toda la tecnología, no tiene su propia conciencia. Si se convertirá en una fuerza para bien o para mal depende del hombre. […] Hemos decidido ir a la luna. Elegimos ir a la luna en esta década y hacer lo demás, no porque sean metas fáciles, sino porque son difíciles, porque ese desafío servirá para organizar y medir lo mejor de nuestras energías y habilidades, porque ese desafío es un desafío que estamos dispuestos a aceptar, uno que no queremos posponer, y uno que intentaremos ganar, al igual que los otros.

¡Claro que sí! A eso es a lo que me refiero. ¿Dónde está ese líder? ¿Ese hombre o mujer que nos interne con osadía en el siglo XXI, utilizando la tecnología para la mejora común y dispuesto a apostar su reputación y honor en pos de la consecución de esa misión sagrada, un hombre que dé muestras de un valor y una determinación enormes y de la convicción necesaria para hacer realidad su sueño? Sólo mediante una coordinación impecable de los esfuerzos entre los ámbitos gubernamental y académico y el sector privado conseguiremos progresar. La clave para que el Proyecto Manhattan para Internet resulte efectivo pasará por imprimirle una entusiasta sensación de urgencia proporcional a la enormidad y la trascendencia de la labor que tenemos por delante. El reloj sigue sonando y no hay mejor momento que el presente para llevar esta idea buen puerto.

Consideraciones finales

La mejor manera de predecir el futuro es inventarlo.

ALAN KAY, Xerox Parc

En lo tocante a las amenazas tecnológicas dirigidas contra la seguridad de todos, el futuro ya está aquí. Está sentado en un edificio de oficinas en Kiev, predestinado a convertirse en la próxima Innovative *Marketing*. Está en el ordenador de ese chaval que tienes sentado al lado en la biblioteca y que se dedica a construir la próxima Silk Road o el nuevo Assassination Market. Está en ese edificio gubernamental de diez plantas en esa capital extranjera donde a diario miles de espías digitales acuden a trabajar, con la consigna de robarte tus secretos corporativos. Está en el garaje de ese *biohacker* marginado que está cansado de que se metan con él en la escuela y ahora trama su venganza bioterrorista. Está en el centro comercial más próximo, vendiendo drones cuadricópteros, ajeno a si se utilizarán para transportar armas por encima de los muros de las prisiones o de las verjas de un aeropuerto. Está disponible a través de ese sitio web que vende maquetas de aviones a reacción capaces de volar de manera autónoma, aviones que los terroristas pueden cargar con explosivos y lanzar contra un edificio repleto de gente. Ese futuro ya ha llegado. Todas las advertencias e indicadores están aquí. La amenaza es seria y ahora es el momento de prepararse; ten por seguro que los delincuentes, terroristas y otros malhechores ya lo han hecho.

Como hemos visto, todo está conectado y todos somos vulnerables. Pero no todo está perdido; aún nos queda un cierto margen de actuación, tal como se ha esbozado en este capítulo y en el precedente. Por mucho que optemos por enterrar la cabeza bajo la arena, si no plantamos cara a este problema, no desaparecerá por sí solo; al contrario, se agravará. Los desafíos que debemos salvar son importantes, y cada vez se amplían más. No se trata sólo de cuentas bancarias pirateadas o de fotografías privadas robadas. Ni tampoco de preservar el control y la privacidad sobre la multiplicidad de dispositivos que pueblan nuestras vidas. Se trata de salvaguardar nuestro futuro tecnológico y entender qué es lo siguiente. Tal como nos recuerda Marshall McLuhan: «Con cada nueva tecnología no sólo cambia la fotografía, sino también el marco».

Las manipulaciones del mañana afectarán a nuestros automóviles, sistemas GPS, dispositivos médicos implantables, televisores, ascensores, contadores inteligentes, cámaras vigilabebés, líneas de montaje y robots de cuidado personal. Con setenta y nueve octillones de conexiones nuevas posibles habilitadas a través del protocolo IPv6 y la Internet de las Cosas, todos los objetos físicos podrán piratearse, incluidas todas las pantallas de tu vida. Y pese a ello, en la actualidad carecemos de modelos viables para una computación segura y fiable, un fracaso evidente de una sociedad edificada sobre y manejada por ordenadores. Nada nos demuestra que podamos

confiar en el código que gobierna nuestras vidas y gestiona nuestro mundo. Precisamente por ese motivo quienes controlen el código controlarán el mundo, para bien y para mal. A partir de ahí, deberemos lidiar con nuevas armas biológicas, ADN manipulado y usurpación de identidades genéticas y biométricas, por no hablar ya de la facilidad con la que se subvierten los algoritmos de caja negra y los sistemas de inteligencia artificial. Corren tiempos exponenciales y, aunque es fácil desdeñar los robots asesinos autónomos y las AI malévolas a lo Skynet, por considerarlas una fantasía futurista propia de la ciencia ficción, tal como nos recuerda George Carlin: «El futuro pronto será una cosa del pasado».

En un mundo en el que todas las infraestructuras y todos los sistemas esenciales se manejan mediante ordenadores, sería fácil calificar nuestra profunda falta de seguridad tecnológica como un mero problema computacional. Pero no sólo tenemos un problema de tecnologías de la información. Puesto que la tecnología está entretejida con todo el entramado de nuestras vidas modernas, también tenemos un problemas social, un problema personal, un problema económico, un problema de salud, un problema de fabricación, un problema de seguridad pública, un problema gubernamental, un problema de transporte, un problema energético, un problema de privacidad y un problema de derechos humanos. No nos queda más remedio que ganar esta batalla por el alma de nuestras propias tecnologías porque, francamente, la alternativa es demasiado espeluznante para planteársela siquiera. Ha llegado el momento de pasar a la acción.

Y en este sentido, ha llegado también el momento de reconsiderar por completo lo que todos damos por sentado en este mundo tecnológico moderno en el que vivimos y poner en tela de juicio nuestra dependencia de tantas máquinas ubicuas que tan pocos de nosotros entendemos. Pero tal empresa no debe acometerse espoleados por una tecnofobia ciega ni por una deferencia a nuestros antepasados luditas, sino como medida de sentido común, siendo plenamente conscientes del inmenso potencial que auguran las tecnologías exponenciales. La innovación avanza imparable y el ritmo al cual se producen cambios tecnológicos aumenta día tras día. Hemos alcanzado un punto de inflexión, un momento puntual en el tiempo que exige nuestra atención más inmediata y concentrada. El vigesimonoveno día del proverbial estanque se aproxima a gran velocidad y, como ocurre con todo lo exponencial, nuestra ventana para actuar de manera responsable y sensata se está cerrando a toda prisa. Hay una manera de continuar avanzando frente a las amenazas tecnológicas que se ciernen sobre nosotros. Movilizando a los ciudadanos corrientes y recuperando el control de nuestros dispositivos y tecnologías, todos estaremos en disposición de utilizar estas herramientas de la manera más provechosa. En otras palabras, las herramientas para cambiar el mundo están en manos de todos. Cómo las utilicemos no es sólo cosa mía; es cosa de todos. Esa versión mejor del futuro, la que todos anhelamos, no aparecerá por arte de magia. Exigirá una determinación, un esfuerzo y una lucha tremendos por parte de todos. Pero con trabajo duro, no sólo será posible sobrevivir al progreso, sino

prosperar con él en una medida previamente inconcebible. Ése es el mundo en el que yo quiero vivir.

Apéndice

Todo está conectado. Todos somos vulnerables

A lo largo de este libro hemos analizado las amenazas tecnológicas latentes a las que se enfrenta la sociedad y hemos explorado diversos modos de reducir sistemáticamente estos riesgos. El protocolo de **ACTUALIZACIÓN**, descrito a continuación, recoge algunas estrategias prácticas cotidianas que puedes aplicar para protegerte, para proteger tu negocio y para proteger a tus seres queridos de los peligros tecnológicos más comunes hoy en día. Sigue estos sencillos pasos (el equivalente digital a cerrar la puerta de tu casa con llave y a no dejarte las llaves puestas en el coche) y evitarás más del 85 por ciento de las amenazas digitales que permean nuestras vidas a diario[1].

ACTUALIZACIONES FRECUENTES.

La mayoría de los programas de *software* están repletos de errores o *bugs*. Los piratas informáticos y otros agentes aprovechan estas vulnerabilidades para colarse en tu ordenador y otros servicios, robarte el dinero y causar estragos en general. Evita estos problemas actualizando de manera automática el *software* de tus sistema operativo, tus programas informáticos y las aplicaciones del móvil. Presta especial atención a los navegadores, módulos *plug-in*, reproductores multimedia, *Flash* y Adobe Acrobat, objetivos predilectos de los malhechores que pretenden estafarte. Si no actualizas tus dispositivos automáticamente, quedarán expuestos a ataques a causa de problemas que podrían haberse evitado sólo con haber actualizado el *software*.

CONTRASEÑAS.

Se recomienda que las contraseñas sean largas (de veinte o más dígitos) y que contengan letras en mayúsculas y minúsculas, además de símbolos y espacios. Pese a que todos lo hemos escuchado un millón de veces, la robustez de una contraseña es uno de los factores clave para proteger tus cuentas. Además, hay que cambiar las contraseñas con frecuencia. No deberías bajo ningún concepto utilizar la misma contraseña para sitios distintos. Hacerlo implica que, una vez que los piratas informáticos obtienen acceso a tus credenciales de inicio de sesión, pueden utilizarlas en múltiples lugares, desde tus redes sociales hasta tu cuenta bancaria. Ahora bien, memorizar largas contraseñas únicas para cada cuenta y sitio web de tu vida excede

lo que la mente humana puede gestionar. Por suerte, hay un montón de «monederos» o gestores de contraseñas que pueden hacer que este proceso resulte relativamente indoloro. Es sabido que los delincuentes también han creado sus propios gestores de contraseñas en un intento por engatusarte para que les entregaras tus joyas de la corona digitales. Así que te recomiendo utilizar sólo los gestores de empresas reputadas y establecidas en el sector, como 1Password, LastPass, KeePass y Dashlane, la mayoría de los cuales funcionan tanto en ordenadores como en teléfonos inteligentes y tabletas. Además, muchos servicios, como Google, iCloud, Dropbox, Evernote, PayPal, Facebook, LinkedIn y Twitter permiten utilizar autenticación de doble factor, que consiste en enviarte una contraseña única aparte cada vez que te conectas, normalmente mediante un mensaje SMS o aplicación directamente al teléfono móvil. El uso de autenticación de doble factor comporta que, si te roban la contraseña, no pueda utilizarse sin el segundo factor de autenticación (el acceso físico a tu dispositivo móvil en sí).

DESCARGA.

Descarga *software* sólo de sitios oficiales (como la App Store de Apple o directamente del sitio web verificado de la empresa). Sé escéptico frente a las tiendas de aplicaciones no oficiales y los sitios de terceros que albergan *software* «gratuito». Además, evita los contenidos pirateados y el *software* ampliamente disponible en redes entre pares P2P, ya que con frecuencia contiene *software* malicioso y virus. Los ajustes de configuración tanto del sistema operativo Windows como Mac te ayudarán a crear una «lista blanca», de manera que sólo se pueda ejecutar *software* aprobado de fabricantes identificados en tu máquina. Pese a que proceder de este modo no te garantizará la seguridad del *software*, sí que puede reducir enormemente el riesgo de infección. Presta mucha atención a las aplicaciones y sus permisos. Son «gratuitas» por un motivo y el precio suele ser tu privacidad. Si una aplicación de una linterna te dice que necesita acceder a tu localización y contactos, huye corriendo.

ADMINISTRADOR.

Las cuentas de administrador deben manejarse con precaución. Tanto Windows como Apple permiten a los usuarios definir los privilegios de cada cuenta, si bien los administradores son siempre los que más tienen. Pese a que necesitarán configurar una cuenta de administrador en tu ordenador, no debería ser tu cuenta por omisión para trabajar y navegar por Internet a diario. En su lugar, crea una cuenta de usuario estándar para realizar la mayor parte del trabajo diario. Si estás conectados con privilegios de administrador y por casualidad haces clic en un archivo infectado o te

descargas un virus, el *software* malicioso cuenta con privilegios absolutos para ejecutarse e infectar tu máquina. En cambio, si estás conectado como un usuario general y te infectas, a menudo el virus, troyano o gusano requerirá permisos específicos para ejecutarse, lo cual te alertará de que hay algún problema. Utiliza siempre el ordenador como usuario general a menos que precises conectarte como administrador para llevar a cabo una tarea concreta, como actualizar un programa de una fuente de confianza que estés instalando conscientemente.

APAGA EL ORDENADOR.

Apaga el ordenador cuando no lo utilices. El simple acto de apagar el ordenador mientras duermes reducirá automáticamente tu perfil de amenaza en un tercio, porque los ladrones no pueden acceder a tu máquina cuando no la usas ni está conectada a Internet. Asimismo, desactiva los servicios y conexiones de tu teléfono inteligente cuando no los utilices. Mantener el Bluetooth, la Wi-Fi, NFC y el acceso inalámbrico al móvil en todo momento proporciona vías adicionales de ataque, que los ladrones pueden utilizar para vulnerar tu teléfono, propagar *software* malicioso y robar datos. Además, mantener el Wi-Fi encendido permite a los comerciantes y anunciantes rastrearte continuamente en el mundo físico, invadiendo aún más tu privacidad. Activa sólo estos servicios cuando los necesites.

ENCRIPTACIÓN.

Encripta tu vida digital y protege tus datos tanto mientras permanecen guardados localmente como mientras circulan por la Red. Tanto Windows como Mac incluyen programas gratuitos para encriptar todo el disco duro (BitLocker y FileVault, respectivamente). Encriptar tu disco duro implica que los demás no puedan acceder a su contenido si lo pierdes o te lo roban. También conviene que encriptes el tráfico por Internet utilizando una red privada virtual (VPN), sobre todo cuando usas una red Wi-Fi pública como las de los aeropuertos, universidades, conferencias y cafeterías, objetivos habituales de piratas informáticos y ladrones. En cuanto a tu teléfono, también conviene encriptarlo, porque los dispositivos móviles actuales pueden contener tanta o más información personal que los ordenadores portátiles. Utiliza siempre una contraseña en el teléfono móvil y plantéate habilitar la seguridad biométrica, como la tecnología de huella digital Touch ID de Apple. Utilizar una contraseña en la última versión de iOS y Android no sólo garantiza que nadie más pueda acceder a tu teléfono y a los datos que contiene en tu ausencia, sino que, además, encripta por completo el dispositivo y con ello añade una capa adicional de privacidad y seguridad.

Consejos de seguridad adicionales.

Si sigues al pie de la letra el protocolo **UPDATE** anterior, evitarás más del 85 por ciento de las amenazas. Para reforzar más tu seguridad, observa los consejos siguientes.

1. Usa el correo electrónico con sentido común. Por regla general, recela de cualquier solicitud de hacer clic en un enlace o abrir un archivo adjunto, incluso aunque parezca proceder de alguien a quien conoces. Los delincuentes son expertos en engatusar al público general con titulares irresistibles, como «clica aquí» para ver las asombrosas fotografías de una estrella de cine desnuda. Los ataques de *phishing* funcionan únicamente porque personas confiadas hacen clic en archivos y enlaces que parecen realistas o son tentadores, pero en realidad contienen una carga maliciosa que infectará tu máquina. Si dudas, pregunta al supuesto remitente si realmente te ha enviado el correo electrónico (¡nunca contestes al mensaje de correo!). Y no, el príncipe de Nigeria no se pone en contacto contigo personalmente para ofrecerte un modo viable de hacerte rico.
2. Las unidades de USB son uno de los medios más habituales para propagar *software* malicioso y otros virus informáticos (el Departamento de Defensa incluso ha prohibido su uso). Como norma general, no aceptes una memoria USB de un desconocido (ni siquiera de una persona a quien conozcas bien) y nunca la conectes en tu ordenador sin primero escanearla en busca de virus. Desactiva la función de «ejecutar automáticamente» las llaves USB en el ordenador para asegurarte de que los virus no se ejecuten automáticamente y te infecten. Y el mismo consejo se aplica a los discos duros USB externos e incluso a los *smartphones* de otras personas.
3. Haz copias de seguridad de tus datos con frecuencia. Puedes guardar las copias de seguridad en un disco duro externo mediante herramientas incorporadas en el sistema operativo, como Time Machine de Mac o Windows Backup. Otra opción es utilizar proveedores en la nube como Carbonite, Backblaze y SpiderOak. Si te decantas por esta última alternativa, conviene que encriptes los datos antes de cargarlos en la nube como medida adicional de protección. Además, recuerda hacer siempre múltiples copias de seguridad de tus datos. Reserva uno o varios discos físicos para hacerlas y asegúrate de guardar al menos uno de ellos en otro lugar para que si se produce algún desastre, incendio o si te roban, tengas una copia de seguridad de tus datos a buen recaudo.
4. Tápate bien. Por desgracia, a los piratas informáticos, delincuentes y espías les es muy fácil acceder a todas las cámaras conectadas a Internet que hay en tu vida, tanto la del ordenador como la del teléfono inteligente o la Tablet. Cuando no utilices la cámara, tapa la lente. Un simple *Post-it* o un trozo de cinta adhesiva servirá y te protegerá de los mirones.
5. Es recomendable que restrinjas la navegación por sitios web delicados, como el de tu entidad bancaria o las páginas donde compras, a dispositivos de tu pertenencia y a una red de tu confianza. Tanto del teléfono de un amigo, un ordenador público o a través del Wi-Fi gratuito de un bar, tus datos podrían ser robados o copiados. Recela especialmente de los ordenadores situados en zonas comunitarias o con mucho tráfico, como las salas de espera de los aeropuertos, pues se cuentan entre las dianas favoritas de los delincuentes, que acostumbran a instalar *software* malicioso y registradores de pulsaciones del teclado en zonas donde se congrega gente de negocios.
6. Reflexiona antes de compartir algo en las redes sociales. Los delincuentes, desde acosadores hasta ladrones, supervisan de manera rutinaria las redes sociales en busca de información. Publicar itinerarios de trabajo puede indicar a los cacos que te ausentarás de tu domicilio durante dos semanas en las vacaciones… y suponerte un problema.
7. Utiliza el programa cortafuegos incorporado de tu sistema operativo, disponible tanto en Windows como en Mac, para bloquear las conexiones no deseadas en tu máquina y activa el «modo encubierto» o «modo furtivo» para dificultar aún más a los piratas informáticos y *bots* de la delincuencia automatizas que te localicen online.

NOTA: Tanto las amenazas como las herramientas para protegerte en Internet cambian con frecuencia. Para obtener información adicional, visita

www.futurecrimes.com (en inglés).

Agradecimientos

Una cosa más…

STEVE JOBS

Un proyecto de esta magnitud nunca puede ser la obra de un solo individuo. En este sentido, estoy en deuda con un amplio número de personas, tanto por el apoyo como por la colaboración que me han brindado durante la creación de este volumen, con mención especial a mi agente literario, Richard Pine, de InkWell Management. Desde muy al principio, Richard vio el potencial de *Future Crimes* y depositó su fe en mí para que lo escribiera, accediendo generosamente a servirme de *sherpa*, mentor y amigo mientras me internaba en el mundo de la edición. A lo largo del camino me hizo varios regalos, pero quizá el mejor de todos fuera presentarme al magnífico equipo de Doubleday, entre quienes destacan su editor jefe, Bill Thomas, y mi propia revisora, Melissa Danaczko. El entusiasmo y el apoyo que Bill me transmitió con *Future Crimes* fueron excepcionales. Y lo mismo vale para todas aquellas personas con quienes tuve el privilegio de trabajar en Doubleday, incluidas entre ellas Alison Rich, Joe Gallagher, Kim Thornton, Margo Shickmanter y Maria Massey. Sin duda, mi reconocimiento más absoluto y profundo está dirigido a Melissa Danaczko, quien me alentó en cada paso del camino a lo largo del proceso de escritura y revisión. Es brillante, divertida y generosa. Trabajó fines de semana y noches e incluso se saltó reuniones familiares a causa de este libro. Sin Melissa, esta obra sencillamente nunca habría llegado a buen puerto, motivo por el cual le estaré eternamente agradecido.

Deseo expresar asimismo todo mi respeto a todas las personas que accedieron amablemente a revisar las galeradas del libro y a plantearme sus críticas y comentarios: mi más sincero agradecimiento por sacar tiempo de vuestros apretados horarios para hacerlo. En concreto, deseo expresar mi gratitud a Peter Diamandis, Ray Kurzweil, Kevin Kelly, Daniel Pink, David Eagleman, Christopher Reich, el presidente de la Interpol Khoo Boon Hui, Ed Burns, Frank Abagnale y P. W. Singer. A Sarah Stephens y Adam Kaslikowski, gracias por las incontables horas que invertisteis leyendo las primeras versiones de *Future Crimes* y por las interesantísimas opiniones que me participasteis sobre la obra a lo largo de su elaboración. También me he beneficiado enormemente de los sabios consejos que con liberalidad compartieron conmigo autores reputados, quienes accedieron de manera altruista a ayudar a un novato a entender este medio sin más razón que la de ser personas generosas, amables y asombrosas. Por todo ello, vaya mi más sincera gratitud a Daniel Suarez, Ramez Naam y Jane McGonigal.

Escribir un libro no es una empresa fácil, no sólo por las incontables horas que te mantiene alejado de tus amistades y familiares, sino porque el proceso de escritura te obliga a imponerle el libro a los demás por el mero hecho de formar parte de tu vida.

Por soportarme y ofrecerme su consejo acerca de una cantidad infinita de títulos de libros, subtítulos, portadas, investigación y opciones de estructura, quiero expresar mi agradecimiento a Jacque Murphy, Tarun Wadhwa, Mikhail Grinberg, Daniel Teweles y Kelsey Segaloff, así como a Brad, Steve, Adam, Carol, Monte, Jacqueline, Noni, Bob, Hanna, Mark y Jonathan. Estoy en deuda con Paul Saffo, Chris Meyer, Joe Polish, Marcus Shingles, Steven Kotler, Jonathan Knowles, Sheryl Rapp, Eileen Bartholomew, Dave Blakely, Bill Eggers, Diane Francis y Cody Rapp por su apoyo explícito a *Future Crimes* y por darme tantas buenas ideas acerca de cómo compartir la información contenida en este libro con otras personas. También me gustaría expresar mi gratitud a los expertos en la materia que me ayudaron con parte del contenido técnico de este libro, incluidos Andrew Hessel sobre biología sintética, Alaina Hardie sobre robótica, Don Bailey sobre la Internet de las Cosas, Emeline Paat-Dahlstrom y Mark Ciotola sobre el espacio, y Andrew Fursman y Landon Downs sobre computación cuántica. Gracias también a Keith Blount, fundador de Literature & Latte's Scrivener, el programa de escritura más maravilloso que existe. Sin Scrivener, habría sido prácticamente imposible organizar los centenares de casos y los miles de páginas de materiales de investigación empleados para redactar este libro.

Deseo asimismo extender mi agradecimiento a mis amigos y colegas en los cuerpos de seguridad, con quienes he compartido multitud de investigaciones, aventuras y buenos momentos a lo largo de los años, incluidos Michael Holstein, Bernhard Otupal, Rainer Buhrer, Paul Gillen, Mick Moran, Andrew Smith, Skukesha Goldberg, Jim Hirt, Bobby Weaver, Robert Rodriguez, Steven Chabinsky y Kathy O'Toole. A mis aliados en la lucha por reforzar la seguridad mundial común, incluidos entre ellos Roderick Jones, Justin Somaini, Tom Kellermann, Matt Wollman, Bradford Davis y Steve Santorelli, gracias por vuestro trabajo.

Tengo el privilegio de impartir clases en la facultad de la Singularity University, una institución educativa fascinante con la misión de utilizar las tecnologías de la próxima generación para afrontar los mayores desafíos a los que se enfrenta el mundo. Allí colaboro con algunas de las personas más talentosas que he conocido en toda mi vida, tanto personal docente como personal en general, estudiantes y alumnos profundamente comprometidos a cambiar este mundo para bien. Tengo el honor de contarme entre ellos y deseo dar las gracias a Rob Nail por su liderazgo a la hora de impulsarnos a avanzar de manera exponencial.

Por último, esta lista de agradecimientos estaría incompleta si no reconociera el apoyo de mi familia, quienes me han servido de pilar para lograr todo lo que he conseguido en la vida y me han inculcado la importancia de luchar por que haya justicia en el mundo. Mi aprecio y gratitud más profundos hacia todos vosotros.

MARC GOODMAN es un estratega global, autor y consultor enfocado en el impacto disruptivo del avance de las tecnologías en seguridad, negocios y asuntos internacionales. Durante los últimos veinte años, ha construido su experiencia en amenazas de seguridad de próxima generación como el ciberdelito, el ciberterrorismo y la guerra de información, trabajando con organizaciones como Interpol, las Naciones Unidas, la OTAN, el Departamento de Policía de Los Ángeles y el Gobierno de los Estados Unidos. Marc frecuentemente aconseja a líderes de la industria, ejecutivos de seguridad y diseñadores de políticas mundiales sobre riesgos e inteligencia cibernéticos transnacionales y ha operado en casi setenta países de todo el mundo.

Marc es fundador del Future Crimes Institute, creado para inspirar y educar a otros sobre las consecuencias en cuanto a la seguridad y el riesgo de las nuevas tecnologías emergentes. Marc también sirve como el asesor de Seguridad Global y Presidente de Política y Derecho en Silicon Valley Universidad de Singularity, con la NASA y Google patrocinando la utilización de la ciencia y la tecnología avanzada para afrontar los grandes retos de la humanidad. Las actuales áreas de investigación de Marc incluyen las implicaciones de seguridad de las tecnologías exponenciales como la robótica, la inteligencia artificial, la revolución de los datos sociales, la biología sintética, los mundos virtuales, la genómica, la computación ubicua y los servicios basados en la localización.

Durante más de una década, Marc trabajó extensamente con la INTERPOL, la Organización Internacional de Policía Criminal, con sede en Lyon, Francia, como

Asesor Principal del Comité Directivo de la organización en Tecnología de la Información del crimen. En esa capacidad, Marc ha entrenado a las fuerzas policiales en Oriente Medio, África, Europa, América Latina y Asia y ha presidido numerosos grupos de expertos de INTERPOL sobre amenazas de seguridad de próxima generación.

Marc ha escrito más de una docena de artículos de revistas y diez capítulos de libros sobre una variedad de amenazas de seguridad emergentes, entre ellas la cibercriminalidad, la bioseguridad y la protección de las infraestructuras críticas. Obras representativas han sido publicados por la Harvard Business Review, The Atlantic, Forbes, The Economist, Harvard Revista de Derecho y Tecnología, Oxford University Press, revisión de la inteligencia de Jane, la American Bar Association, la ejecución Boletín Ley del FBI, el Instituto de Ingenieros en Electricidad y Electrónica (IEEE).

Marc tiene una Maestría en Administración Pública de la Universidad de Harvard y una Maestría en Ciencias en Gestión de Sistemas de Información de la London School of Economics. Además, se ha desempeñado como Fellow en la Universidad de Stanford Centro para la Seguridad y la Cooperación Internacional y es un distinguido profesor visitante en el Laboratorio MediaX de Stanford. Marc es frecuentemente entrevistado por la prensa, habiendo sido presentado por CNN, ABC, NBC, BBC, Fox News, The Guardian, Le Monde y PBS, entre otros.

Notas

[1] Michael Weissenstein. «Mexico’s Cartels Build Own National Radio System». En: *Associated Press*, 27 de diciembre de 2011. <<

[1] Mat Honan. «How Apple and Amazon Security Flaws Led to My Epic Hacking». En: *Wired*, 6 de julio de 2012; Mat Honan. «Kill the Password: Why a String of Characters Can’t Protect Us Anymore». En: *Wired*, 15 de noviembre de 2012. <<

[2] Peter Diamandis. «Abundance Is Our Future». Conferencia TED Talk, febrero de 2012. <<

[3] Deloitte Consulting. *Sub-Saharan Africa Mobile Observatory 2012*. 4 de febrero de 2014. <<

[4] Marc Goodman. «The Power of Moore’s Law in a World of Geotechnology». En: *National Interest*, enero/febrero de 2013. <<

[5] Amy Harmon. «Hacking Theft of $10 Million from Citibank Revealed». En: *Los Angeles Times*, 19 de agosto de 1995. <<

[6] Jason Kersten. «Going Viral: How Two Pakistani Brothers Created the First PC Virus». En *Mental Floss*, noviembre de 2013. <<

[7] Para obtener una fascinante y entretenida semblanza de Amjad y Basit Farooq y conocer la historia de su virus informático, *véase*: Mikko Hypponen. «Fighting Viruses and Defending the Net». Conferencia TED Talk, julio de 2011. <<

[8] Byron Acohido. «Malware Now Spreads Mostly Through Tainted Websites». En: *USA Today*, 4 de mayo de 2013. <<

[9] Brian Fung. «911 for the Texting Generation Is Here». En: *Washington Post*, 8 de agosto de 2014. <<

[10] Nicole Perlroth. «Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt». En: *New York Times*, 31 de diciembre de 2012. <<

[11] Kaspersky Lab. *Global Corporate IT Security Risks: 2013*. Mayo de 2013. <<

[12] «Online Exposure». En: *Consumer Reports*. Junio de 2011. <<

[13] «Gartner Says Worldwide Security *Software* Market Grew 7.9 Percent in 2012». Gartner Newsroom, 30 de mayo de 2013; Steve Johnson. «Cybersecurity Business Booming in Silicon Valley». En: *San Jose Mercury News*, 13 de septiembre de 2013. <<

[14] Imperva. *Hacker Intelligence Initiative, Monthly Trend Report #14*. Diciembre de 2012. <<

[15] Tom Simonite. «The Antivirus Era Is Over». En: *MIT Technology Review*, 11 de junio de 2012. <<

[16] Verizon. *2013 Data Breach Investigations Report*. <<

[17] Trustwave. *Trustwave 2013 Global Security Report*. <<

[18] Verizon RISK Team. *2012 Data Breach Investigation Report*, pág. 3. <<

[19] Ibíd., pág. 51. <<

[20] Mark Jewell. «T. J. Maxx Theft Believed Largest *Hack* Ever». Associated Press, 30 de marzo de 2007. <<

[21] Julianne Pepitone. «5 of the Biggest Ever Credit Card *Hacks*». CNN, 12 de enero de 2014. <<

[22] Ross Kerber. «Banks Claim Credit Card Breach Affected 94 Million Accounts». *New York Times*, 24 de octubre de 2007. <<

[23] Ponemon Institute, página de inicio de su sitio web en 2014: http://www.ponemon.org. <<

[24] Byron Acohido. «Experts Testify on True Cost of Target Breach». *USA Today*, 5 de febrero de 2014. <<

[25] Robin Sidel y Andrew R. Johnson. «Data Breach Sparks Worry». En: *Wall Street Journal*, 30 de marzo de 2012. <<

[26] Ponemon Institute (esponsorizado por Symantec). *2013 Cost of Data Breach Study: Global Analysis*. Mayo de 2013. <<

[1] Graeme Baker. «Schoolboy *Hacks* into City's Tram System». En *Telegraph*, 11 de enero de 2008. <<

[2] Chuck Squatriglia. «Polish Teen *Hacks* His City's Tram, Chaos Ensues». *Wired*, 11 de enero de 2008. <<

[3] *Ibíd.* <<

[4] Clay Wilson. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service, 9 de enero de 2008, pág. 25. <<

[5] Brian Prince. «Almost 70% of Infrastructure Companies Breached in Last 12 Months: Survey». En: *Security Week*, 14 de julio de 2014. <<

[6] «*Hackers* “Hit” US *Water* Treatment Systems». BBC, 21 de noviembre de 2011. <<

[7] Martha Stansell-Gamm. «Interview: Martha Stansell-Gamm». En: *Frontline*, febrero de 2001; Sean Silverthorne. «Feds Bust Kid *Hacker*». En: *ZDNet*, 18 de marzo de 1998. <<

[8] Tony Smith. «*Hacker* Jailed for Revenge Sewage Attacks». En: *Register*, 31 de octubre de 2001. <<

[9] Anna Mulrine. «CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyber Attack». En: *Christian Science Monitor*, 9 de junio de 2011. <<

[10] Discurso del Presidente del Consejo de Asesores Económicos y de la Oficina de Electricidad del Departamento de Energía de Estados Unidos. *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages Report*. Agosto de 2013. <<

[11] Edward J. Markey y Henry A. Waxman. *Electric Grid Vulnerability Report*, 21 de mayo de 2013. <<

[12] Siobhan Gorman. «Electricity Grid in U. S. Penetrated by Spies». En: *Wall Street Journal*, 8 de abril de 2009. <<

[13] Jack Cloherty. «Virtual Terrorism: Al Qaeda Video Calls for “Electronic Jihad”». En: *World News*, 22 de mayo de 2012. <<

[14] Barton Gellman. «Cyber Attacks by Al Qaeda Feared». En: *Washington Post*, 27 de junio de 2002. <<

[15] Darlene Storm. «*Hackers* Exploit SCADA Holes to Take *Full* Control of Critical Infrastructure». En: *Computerworld*, 15 de enero de 2014; Vortrag: SCADA StrangeLove 2, http://events.ccc.de/. <<

[16] Shodan HQ, página de inicio, acceso realizado el 9 de febrero de 2014: http://www.shodanhq.com. <<

[17] «Cyber War: Sabotaging the System». En: *60 Minutes*, 6 de junio de 2011. Para consultar el punto de vista de los delincuentes, *véase* David Shamah. «*Hack* Attacks on Infrastructure on the Rise, Experts Say». En: *Times of Israel*, 30 de enero de 2014. <<

[18] Barack Obama. «Remarks by the President on Securing Our Nation’s Cyber Infrastructure». Oficina del Secretario de Prensa de la Casa Blanca, 29 de mayo de 2009. <<

[19] «War in the Fifth Domain». En: *Economist*, 5 de julio de 2010. <<

[20] Phil Lapsley. «The Definitive Story of Steve Wozniak, Steve Jobs, and Phone Phreaking». En: *Atlantic*, 20 de febrero de 2013. <<

[21] Kevin D. Mitnick y William L Simon. *El arte de la intrusión* (trad. de Inmaculada González Cerezo). Madrid: RA-MA S. A. Editorial y Publicaciones, 2006. <<

[22] Jonathan Littman. «The Last *Hacker*». En: *Los Angeles Times*, 12 de septiembre de 1993. <<

[23] «Adobe *Hack*: At Least 38 Million Accounts Breached». BBC, 30 de octubre de 2013. <<

[24] Brian Krebs. «Adobe to Announce Source Code, Customer Data Breach». En: *Krebs on Security*, 3 de octubre de 2013. <<

[25] Darlene Storm. «AntiSec Leaks Symantec pcAnywhere Source Code After $50K Extortion Not Paid». En: *Computerworld*, 7 de febrero de 2012. <<

[26] La Haya, *Evaluación de la amenaza de la delincuencia organizada: la Mafia italiana*, Información Pública de la Europol, junio de 2013; Nir Kshetri. *The Global Cybercrime Industry: Economic, Institutional, and Strategic Perspectives*. London: Springer, 2010, pág. 1; Chuck Easttom, *Computer Crime, Investigation, and the Law*. Boston: Cengage Learning, 2010, pág. 206. <<

[27] Mark Milian. «Top Ten Hacking *Countries*». En: *Bloomberg*, 23 de abril de 2013. <<

[28] Brian Krebs. «Shadowy Russian Firm Seen as Conduit for Cybercrime». En: *Washington Post*, 13 de octubre de 2007; Verisign iDefense. *The Russian Business Network: Survey of a Criminal ISP*, 27 de junio de 2007. <<

[29] Trend Micro. *The Business of Cybercrime: A Complex Business Model*. Enero de 2010. <<

[30] Kevin Poulsen. «One *Hacker*'s Audacious Plan to Rule the Black Market in Stolen Credit Cards». En: *Wired*, 22 de diciembre de 2008. <<

[31] James Verini. «The Great Cyberheist». En: *New York Times Magazine*, 10 de noviembre de 2010. <<

[32] John E. Dunn. «Global Cybercrime Dominated by 50 Core Groups, CrowdStrike Report Finds». En: *CSO*, 23 de enero de 2014. <<

[33] En deferencia a Guy Fawkes, el inglés católico que, en 1605, planeó asesinar al rey Jacobo I de Inglaterra y volar por los aires el Parlamento inglés con pólvora. <<

[34] «“The Corrupt Fear Us!” Massive Anonymous “Million Mask March” as It Happened». En: *RT*, 24 de diciembre de 2013; «Anonymous (grupo)», *Wikiquote*. <<

[35] Lauren Turner. «Anonymous *Hackers* Jailed for DDoS Attacks on Visa, MasterCard, and PayPal». En: *Independent*, 24 de enero de 2013. <<

[36] Karol Snapbacks. «Anonymous Explaining Why They Hacked PSN/Sony». YouTube, 22 de abril de 2011; Quinn Norton. «Anonymous Goes After World Governments in Wake of Anti-SOPA Protests». En: *Wired*, 25 de enero de 2012; Lisa Vaas. «Anonymous Bullies Sony and Nintendo over SOPA Support». En: *Naked Security*, 3 de enero de 2012. <<

[37] Quinn Norton. «How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down». En: *Wired*, 3 de julio de 2012. <<

[38] «*Hackers* Take Down Child Pornography Sites». En BBC, 24 de octubre de 2011. <<

[39] Barton Gellman. «The World’s 100 Most Influential People: 2012». En: *Time*, 18 de abril de 2012. <<

[40] «Snowden Leaks: GCHQ “Attacked Anonymous” *Hackers*». BBC, 5 de febrero de 2014. <<

[41] Para consultar información detallada sobre el uso que los terroristas y yihadistas hacen de la tecnología, véase el informe del Equipo Espacial sobre la Ejecución de la Lucha contra el Terrorismo *Lucha contra el uso de Internet con fines terroristas*, mayo de 2011. <<

[42] Paul Tassi. «ISIS Uses “GTA 5” in New Teen Recruitment Video». En: *Forbes*, 20 de septiembre de 2014. <<

[43] Thomas Harding. «Terrorists "Use Google Maps to Hit UK Troops"». En: *Telegraph Online*, 13 de enero de 2007; Caroline McCarthy. «Report: JFK Terror Plotters Used Google Earth». En: *CNET*, 4 de junio de 2007. <<

[44] Jack Kelley. «Terror Groups Hide Behind Web Encryption». En: *USA Today*, 5 de febrero de 2001. <<

[45] Gabriel Weimann. *How Modern Terrorism Uses the Internet*. United States Institute of Peace, Informe especial 116, marzo de 2004. <<

[46] «Search of Tsarnaev’s Phones, Computers Finds No Indication of Accomplice, Source Says». NBC News, 23 de abril de 2013. <<

[47] Equipo Espacial sobre la Ejecución de la Lucha contra el Terrorismo. *Lucha contra el uso de Internet con fines terroristas*, mayo de 2011, pág. 18. <<

[48] Entrevista a Tom Kellermann. «Internet Fraud Finances Terrorism». En: *Discovery News*, 11 de febrero de 2013. <<

[49] Alan Sipress. «An Indonesian's Prison Memoir Takes Holy War into Cyberspace». En: *Washington Post*, 14 de diciembre de 2004. <<

[50] Jeremy Scott-Joynt. «Warning Signs for the Funding of Terror». BBC, 20 de julio de 2005; Gordon Rayner y David Williams. «Revealed: How MI5 Let 7/7 Bombers *Slip* Through Their Fingers». En: *Daily Mail*, 1 de mayo de 2007. <<

[51] Associated Press. «Filipino Police Arrest 4 Suspected AT&T *Hackers*». CBS News, 27 de noviembre de 2011; Somini Sengupta. «Phone Hacking Tied to Terrorists». En: *New York Times*, 26 de noviembre de 2011; Daily *Mail* Reporter. «Four Filipinos Arrested for Hacking AT&T Phone "to Fund Saudi Terror Group"». En: *Daily Mail*, 28 de noviembre de 2011; Jennifer Rowland. «The LWOT: Phone Hacking Linked to Terrorist Activity». En: *Foreign Policy*, 29 de noviembre de 2011. <<

[52] Marc Goodman y Parag Khanna. «The Power of Moore’s Law in a World of Geotechnology». En: *The National Interest*, febrero de 2013. <<

[53] Siobhan Gorman, August Cole y Yochi Dreazen. «Computer Spies Breach Fighter-*Jet* Project». En: *Wall Street Journal*, 21 de abril de 2009. <<

[54] Ernesto Londono. «Pentagon: Chinese Government, Military Behind Cyberspying». En: *Washington Post*, 6 de mayo de 2013. <<

[55] Ellen Nakashima. «Confidential Report Lists U. S. Weapons System Designs Compromised by Chinese Cyberspies». En: *Washington Post*, 27 de mayo de 2013. <<

[56] Marcus Ranum. «Cyberwar Rhetoric Is Scarier Than Threat of Foreign Attack». En: *U. S. News and World Report*, 29 de marzo de 2010. <<

[57] Craig Timberg y Ellen Nakashima. «Chinese Cyberspies Have Hacked Most Washington Institutions, Experts Say». En: *Washington Post*, 20 de febrero de 2013. <<

[58] John Markoff. «Vast Spy System Loots Computers in 103 *Countries*». En: *New York Times*, 28 de marzo de 2009; Omar El Akkad. «Meet the Canadians Who Busted GhostNet». En: *Daily Globe and Mail*, 30 de marzo de 2009; Tom Ashbrook *et al*. «Unmasking GhostNet». En: *On Point with Tom Ashbrook*, WBUR, 2 de abril de 2009, http://onpoint.wbur.org/2009/04/02/*unmasking*-ghostnet. <<

[59] David E. Sanger, David Barboza y Nicole Perlroth. «Chinese Army Unit Is Seen as Tied to Hacking Against U. S.». En: *New York Times*, 18 de febrero de 2013. <<

[60] Mandiant Corp. «APT 1: Exposing One of China’s Cyber Espionage Units». En: *Mandiant*. <<

[61] Michael Riley y Ashlee Vance. «Inside the Chinese *Boom* in Corporate Espionage». En: *Bloomberg Businessweek*, 15 de marzo de 2012. <<

[62] Lisa Daniels. «DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says». En: *Department of Defense News*, 27 de marzo de 2012; David E. Sanger y Mark Landler. «U. S. and China Agree to Hold Regular Talks on Hacking». En: *New York Times*, 1 de junio de 2013. <<

[63] Ian Steadman. «Reports Find China Still Largest Source of Hacking and Cyber Attacks». En: *Wired UK*, 24 de abril de 2013; David Belson. *The State of the Internet*. Informe del tercer trimestre de 2013, Akamai Technologies. <<

[64] Michael Riley. «*Hackers* in China Breach UN, Olympic Committee Networks, Security Firms Say». En: *Bloomberg*, 4 de agosto de 2011. <<

[65] Grupo de Trabajo en materia de Amenazas de la Comisión sobre Seguridad Cibernética del Centro para Estudios Estratégicos e Internacionales, «Threats Posed by the Internet», CSIS, 28 de octubre de 2008. <<

[66] Nicole Perlroth. «In Cyberattack on Saudi Firm, U. S. Sees Iran Firing Back». En: *New York Times*, 23 de octubre de 2012. <<

[67] Jim Finkle. «Exclusive: Insiders Suspected in Saudi Cyber Attack». Reuters, 7 de septiembre de 2012. <<

[68] Reuters. «Aramco Says Cyberattack Was Aimed at Production». En: *New York Times*, 9 de diciembre de 2012. <<

[69] Perlroth. «In Cyberattack on Saudi Firm, U. S. Sees Iran Firing Back». <<

[70] Reuters. «Aramco Says Cyberattack Was Aimed at Production». <<

[71] Siobhan Graham y Danny Yadron. «Iran *Hacks* Energy Firms, U. S. Says». En: *Wall Street Journal*, 23 de mayo de 2013; Michael Lipin. «Saudi Cyber Attack Seen as Work of *Amateur Hackers* Backed by Iran». Voice of America, 25 de octubre de 2012. <<

[72] Jim Finkle y Rick Rothacker. «Exclusive: Iranian *Hackers* Target Bank of America, JP Morgan, Citi». Reuters, 21 de septiembre de 2012. <<

[73] Paul Wagenseil. «Bank of America Website Hit by Possible Cyberattack». NBC News, 19 de septiembre de 2012; Siobhan Gorman y Julian E. Barnes. «Iran Blamed for Cyberattacks». En: *Wall Street Journal*, 12 de octubre de 2012. <<

[74] Nicole Perlroth y Quentin Hardy. «Bank Hacking Was the Work of Iranians, Officials Say». En: *New York Times*, 8 de enero de 2013. <<

[75] La población mundial se sitúa en torno a 7000 millones de personas. Si cada persona del mundo salvo tú levantase el auricular y telefonease a tu banco (transmitiendo, por poner un ejemplo, unos 10 *bytes* por hacer la llamada) y luego colgara inmediatamente y repitiera este procedimiento durante el transcurso del ataque, nos situaríamos en torno a 70 gigabits por segundo. Si alguien en el planeta realmente quisiera hablar con el banco, tendría que colocarse a la cola tras esos 7000 millones de personas. <<

[76] Perlroth y Hardy. «Bank Hacking Was the Work of Iranians». <<

[77] Glenn Greenwald e Ewen MacAskill. «Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data». En: *Guardian*, 11 de junio de 2013; Kevin Drum. «2 Gigantic New NSA Revelations?». *Mother Jones*, 2 de julio de 2013; Catherine Dunn. «10 Most Shocking NSA Revelations of 2013». En: *Fortune*, 27 de diciembre de 2013. <<

[78] «Obama Knew of NSA Spying on Merkel and Approved It, Report Says». Fox News, 27 de octubre de 2013; Catherine E. Shoichet. «As Brazil's Uproar over NSA Grows, US Vows to Work Through Tensions». CNN, 12 de septiembre de 2013. <<

[79] «US Spy Agency “Taped Millions of French Calls”». En: *Local*, 21 de octubre de 2013; Kristen Butler. «NSA Taps Half-Billion German Phone, Data Links per Month: Report». UPI, 30 de junio de 2013; Eric Pfeiffer. «NSA Spied on 124.8 Billion Phone Calls in Just One Month: Watchdog». En: *Yahoo! News*, 23 de octubre de 2013. <<

[80] Te-Ping Chen. «Snowden Alleges U. S. Hacking in China». En: *Wall Street Journal*, 23 de junio de 2013; Lana Lam. «Edward Snowden: US Government Has Been Hacking Hong Kong and China for Years». En: *South China Morning Post*, 13 de junio de 2013; «New Snowden Leak Reveals US Hacked Chinese Cell Companies, Accessed Millions of SMS-Report». En: *RT*, 23 de junio de 2013. <<

[1] Miniwatts *Marketing* Group. «Internet Users in the World», 31 de diciembre de 2013, http://www.internetworldstats.com/. <<

[2] Miniwatts *Marketing* Group. «Internet Growth Statistics». Estadísticas Mundiales de Internet, 6 de febrero de 2013, http:// www.internetworldstats.com/. <<

[3] Miniwatts *Marketing* Group. «Internet Users in the World, Distribution by World Regions». Estadísticas Mundiales de Internet, 5 de febrero de 2014, http://www.internetworldstats.com/. <<

[4] Doug Gross. «Google Boss: Entire World Will Be Online by 2020». CNN, 15 de abril de 2013. <<

[5] Marc Goodman y Parag Khanna. «Power of Moore's Law in a World of Geotechnology». En: *National Interest*, enero/febrero de 2013. <<

[6] Cliff Saran. «Apollo 11: The Computers That Put Man on the Moon». En: *Computer Weekly*, 13 de julio de 2009. <<

[7] Peter Diamandis. «Abundance Is Our Future». Conferencia TED Talk, febrero de 2012. <<

[8] Ray Kurzweil. «The Law of Accelerating Returns». En: *Kurzweil Accelerating Intelligence*, 7 de marzo de 2001. <<

[9] Ray Kurzweil. *The Singularity Is Near: When Humans Transcend Biology*. Nueva York: Penguin, 2006. <<

[10] Evan Andrews. «6 Daring Train Robberies». En: History.com, 21 de octubre de 2013. <<

[11] Brett Leppard. «The Great Train Robbery: How It Happened». En: *Mirror*, 28 de febrero de 2013. <<

[12] Keith Stuart y Charles Arthur. «PlayStation Network *Hack*: Why It Took Sony Seven Days to Tell the World». En: *Guardian*, 5 de febrero de 2014; «Credit Card Alert as *Hackers* Target 77 Million PlayStation Users». En: *Mail Online*, 5 de febrero de 2014. <<

[13] J. Osawa. «As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill». En: *Wall Street Journal*, 9 de mayo de 2011. <<

[14] «Target Now Says up to 110 Million Customers Victimized in Breach». MercuryNews.com, 5 de febrero de 2014; «Pictured: Russian Teen Behind Target Hacking Attack». En: *Mail Online*, 5 de febrero de 2014. <<

[15] Nicole Perlroth y David Gelles. «Russian *Hackers* Amass over a Billion Internet Passwords». En: *New York Times*, 5 de agosto de 2014. <<

[16] Jacques Marescaux *et al*. «Transatlantic Robot-Assisted Telesurgery». En: *Nature*, 29 de mayo de 2001. <<

[17] Phil Johnson. «Curiosity About Lines of Code». En: *IT World*, 8 de agosto de 2012; Saran, «Apollo 11». <<

[18] Steven Siceloff. «Shuttle Computers Navigate Record of Reliability». NASA, 20 de enero de 2011. <<

[19] David McCandless. «Codebases». En: *Information Is Beautiful*, 30 de octubre de 2013; «KIB-Lines of Code (Public)», Google.doc, https://docs.google.com/; Pollwatcher, «Healthcare.gov: 500 Million Lines of Code! That's Insane! Update». En: *Daily Kos*, 22 de octubre de 2013. <<

[20] Cory Doctorow. «Lockdown», basado en un discurso clave en el Congreso de Comunicación Caos celebrado en Berlín en diciembre de 2011. <<

[21] Michelle Delio. «Linux, Fewer Bugs Than Rivals». En: *Wired*, 14 de diciembre de 2004. <<

[22] «Northeast Blackout of 2003». Wikipedia (versión inglesa). <<

[23] Comisión Nacional sobre el Vertido y la Excavación Petrolera en Mar Abierto de BP Deepwater Horizon. «Deep *Water*: The Gulf Oil Disaster and the Future of Offshore Drilling», Informe presentado ante el presidente estadounidense, enero de 2011; «Deepwater Horizon». Wikipedia; Jeremy Repanich. «The Deepwater Horizon Spill by the Numbers». En: *Popular Mechanics*, 10 de agosto de 2010. <<

[24] Gregg Keizer. «Tech Worker Testifies of “Blue Screen Death” on Oil Rig’s Computer». En: *Computerworld*, 23 de julio de 2010; David Hammer. «Oil Spill Hearings: Bypassed General Alarm Doomed Workers in Drilling Area, Technician Testifies». En: *Times-Picayune*, 23 de julio de 2010. <<

[25] Tom Simonite. «Stuxnet Tricks Copied by Computer Criminals». En: *MIT Technology Review*, 19 de septiembre de 2012. <<

[1] Ryan Bradley. «Rethinking Health Care with PatientsLikeMe». En: *Fortune*, 9 de marzo de 2014. <<

[2] Julia Angwin y Steve Stecklow. «Scrapers Dig Deep for Data on Web». En: *Wall Street Journal*, 12 de octubre de 2010. <<

[3] Traducción de un fragmento de la sección de preguntas habituales de PatientsLikeMe.com. <<

[4] Política de privacidad de PatientsLikeMe.com. <<

[5] Angwin y Stecklow. «Scrapers Dig Deep for Data on Web». <<

[6] Cotton Delo. «U. S. Adults Now Spending More Time on Digital Devices Than Watching TV». En: *Advertising Age*, 4 de marzo de 2014. <<

[7] IDC Research. *Always Connected: How Smartphones and Social Keep Us Engaged*. Archivos Públicos de Facebook, 4 de marzo de 2014. <<

[8] Heather Kelly. «By the Numbers: 10 Years of Facebook». CNN, 4 de febrero de 2014. <<

[9] Facebook, Ericsson y Qualcomm. «A Focus on Efficiency», 6, internet.org, 16 de septiembre de 2013: https:// fbcdn-dragon-a.akamaihd.net/. <<

[10] Jose Antonio Vargas. «How an Egyptian Revolution Began on Facebook». En: *New York Times*, 17 de febrero de 2012. <<

[11] Mark Milian. «Google to Merge User Data Across Its Services». CNN, 25 de enero de 2012. <<

[12] Nate Anderson. «Why Google Keeps Your Data Forever, Tracks You with Ads». En: *Ars Technica*, 8 de marzo de 2010. Téngase en cuenta que en la UE sí existen restricciones a durante cuánto tiempo puede almacenar datos Google, la más destacada la llamada «ley de derecho al olvido», que garantiza a las personas el derecho a solicitar que sus datos personales se eliminen del motor de búsqueda. <<

[13] Nate [nombre de usuario], «How Much Is a Petabyte?». En: *The Mozy Blog*, acceso al blog el 5 de marzo de 2014. <<

[14] La empresa ha sido denunciada por todos estos motivos, con resultados diversos. Para consultar informes más detallados sobre el gran número de infracciones de ley por las que se ha denunciado a Google, *véase* www.googlemonitor.com. <<

[15] David Streitfeld. «Google Admits Street View Project Violated Privacy». En: *New York Times*, 12 de marzo de 2013; David Kravets. «An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle». En: *Wired*, 2 de mayo de 2012. <<

[16] Claire Cain Miller. «Google Accused of Wiretapping in Gmail Scans». En: *New York Times*, 1 de octubre de 2013. <<

[17] David Pierce. «The Simpsons May Have the Smartest Thoughts Yet About Google Glass». En: *Verge*, 27 de enero de 2014. <<

[18] Michael Chertoff. «Google Glass, the Beginning of Wearable Surveillance». CNN, 1 de mayo de 2013. <<

[19] PRNewswire. «Facebook Reports Fourth Quarter and *Full* Year 2013 Results». Facebook: Investor Relations, 29 de enero de 2014. <<

[20] Karen Gullo. «Facebook Sued over Alleged Scanning of Private Messages». En: *Bloomberg*, 2 de enero de 2014. <<

[21] Robert McMillan. «Apple Finally Reveals How Long Siri Keeps Your Data». En: *Wired*, 19 de abril de 2013. <<

[22] «What They Know». En: *Wall Street Journal*: http://blogs.wsj.com/wtk/. <<

[23] Adi Robertson. «Angry *Email* Users Can Take Google to Court for Keyword Scanning, Judge Rules». En: *Verge*, 26 de septiembre de 2013. <<

[24] Ibíd., Cooley LLP. «Google's Motion to Dismiss Complaint Memorandum of Points & Authorities». Tribunal de Distrito de Estados Unidos. División de San José, 5 de septiembre de 2013, http://www.consumerwatchdog.org/; Gregory S. McNeal. «It's Not a Surprise That Gmail Users Have No Reasonable Expectation of Privacy». En: *Forbes*, 20 de junio de 2013. <<

[25] Steve Stecklow. «On the Web, Children Face Intensive Tracking». En: *Wall Street Journal*, 17 de septiembre de 2010. <<

[26] Josh Smith. «Children's Online-Privacy Violations Alleged Against McDonald's, General Mills, 3 Others». En: *National Journal*, 22 de agosto de 2012. <<

[27] Comisión Federal de Comercio. «Sony BMG Music Entertainment, a General Partnership Subsidiary of Sony Corporation of America, United States of America (for the Federal Trade Commission)», informe consultado en la web el 6 de marzo de 2014, http://www.ftc.gov/. <<

[28] Roben Farzad. «Google at $400 Billion». En: *Bloomberg Businessweek*, 12 de febrero de 2014. <<

[29] Doug Laney. «To Facebook You’re Worth $80.95». En: *CIO Journal* (blog), *Wall Street Journal*, 3 de mayo de 2012. <<

[30] Joe Nocera. «Will Digital Networks Ruin Us?». En: *New York Times*, 6 de enero de 2014; Jaron Lanier. ¿*Quién controla el futuro*?, Barcelona: Debate, 2014. <<

[31] Lori Andrews. «Facebook Is Using You». En: *New York Times*, 4 de febrero de 2012. <<

[32] Salvador Rodriguez. «Google to Include User Names, Pictures in Ads: Here’s How to Opt Out». En: *Los Angeles Times*, 11 de octubre de 2013. <<

[33] Drew Guarini. «Facebook Finally Axes Controversial “Sponsored Stories”». En: *Huffington Post*, 1 de octubre de 2014. <<

[34] Alexis C. Madrigal. «Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days». En: *Atlantic*, 1 de marzo de 2012. <<

[35] Missy Sullivan. «It’s Not Your Eyes… the Fine Print Is Getting Really, Really Small». En: *Wall Street Journal*, 15 de enero de 2012. <<

[36] Para comprobar que los acuerdos de licencia de rompe y rasga son válidos y legales, *véase*, por ejemplo: *ProCD, Inc. v. Zeidenberg*, *Microsoft v. Harmony Computers*, *Novell v. Network Trade Center* y *Ariz. Cartridge Remanufacturers Ass'n v. Lexmark Int'l, Inc*. también puede ser relevante. <<

[37] Nick Bilton. «Price of Facebook Privacy? Start Clicking». En: *New York Times*, 12 de mayo de 2010; Facebook. «Política de privacidad», acceso realizado el 3 de marzo de 2014, https://www.facebook.com/*full*_data_use_policy. <<

[38] Tom Gardner. «To Read, or Not to Read… the Terms and Conditions: PayPal Agreement Is Longer Than *Hamlet*, While iTunes Beats *Macbeth*». En: *Mail Online*, 22 de marzo de 2012. <<

[39] Guilbert Gates. «Facebook Privacy: A Bewildering Tangle of Options». En: *New York Times*, 21 de mayo de 2010. <<

[40] Jessica Guyn. «With Privacy Battle Brewing, Facebook Won’t Update Policy Right Away». En: *Los Angeles Times*, 5 de septiembre de 2013; Ryan Singel. «Public Posting Now the Default on Facebook». En: *Wired*, 9 de diciembre de 2009; Epic. «Facebook Privacy». En: http://epic.org/privacy/facebook/. <<

[41] «Instagram Seeks Right to Sell Access to Photos to Advertisers». BBC News, 18 de diciembre de 2012. <<

[42] Términos y condiciones de servicio de Google, acceso realizado el 10 de marzo de 2014, http:// www.google.com/; Steve Kovach. «A Lot of People Are Freaking Out over Google Drive for Nothing». En: *Business Insider*, 24 de abril de 2012. <<

[43] «2014: Mobiles “to Outnumber People Next Year,” Says UN Agency». BBC News, 9 de mayo de 2013. <<

[44] Lookout. «Survey Reveals Consumers Exhibit Risky Behaviors Despite Valuing Their Privacy on Mobile Devices», 22 de octubre de 2013. <<

[45] O2. «Making Calls Has Become Fifth Most Frequent Use for a *Smartphone* for Newly Networked Generation of Users». En: *The Blue*, 29 de junio 2012. <<

[46] Meena Hart Duerson. «We’re Addicted to Our Phones: 84% Worldwide Say They Couldn’t Go a Single Day Without Their Mobile Device in Their Hand». En: *Daily News* (edición de Nueva York), 16 de agosto de 2012. <<

[47] Peter Maass y Megha Rajagopalan. «That’s Not My Phone, It’s My Tracker». En: *New York Times*, 13 de julio de 2012. <<

[48] Jeff Jonas. «Your Movements Speak for Themselves: Space Time Travel Data Is Analytic Super-Food». Jeff Jonas .typepad.com, 26 de agosto de 2009. <<

[49] Kai Biermann. «Data Protection: Betrayed by Our Own Data». En: *Die Zeit*, 26 de marzo de 2011. <<

[50] Samsung Tomorrow. «What You May Not Know About GALAXY S4 Innovative Technology», 10 de abril de 2013. <<

[51] Ted Thornhill. «Is Nothing *Off* Limits? Now Google Plans to Spy on Background Noise in Your Phone Calls to Bombard You with Tailored Adverts». En: *Mail Online*, 22 de marzo de 2012. <<

[52] Megan Garber. «Yep, Google Just Patented Background Noise». En: *Atlantic*, 22 de marzo de 2012. <<

[53] Andrea Peterson. «New Facebook Feature Is a Friendly Reminder Your *Smartphone* Can Eavesdrop on You». En: *Washington Post*, 21 de mayo de 2014; Kurt Wagner. «Facebook's New Shazam-Like Tool Knows What You're Watching and Hearing». En: *Mashable*, 21 de mayo de 2014. <<

[54] David de Jong. «Zuckerberg Gains $3.2 Billion as Facebook Soars on Mobile». En: *Bloomberg*, 30 de enero de 2014; Facebook. «Investor Relations», 29 de enero de 2014, http://investor.fb.com/; J. O'Dell. «Facebook's Mobile Moment: Nearly a Billion Mobile Users & Majority of Revenue from Mobile». En: *VentureBeat*, 29 de enero de 2014. <<

[55] «App Store Sales Top $10 Billion in 2013», nota de prensa de Apple, 7 de enero de 2014; Jordan Golson. «Apple Reports Strongest Ever Quarterly Earnings: $13.1 Billion Profit on $57.6 Billion in Revenue in Q1 2014». En: *MacRumors*, 27 de enero de 2014. <<

[56] Emma Barnett. «Angry Birds Company “Worth 5.5bn”». En: *Telegraph*, 8 de mayo de 2012. <<

[57] Violet Blue. «Norton: Android App Skips Consent, Gives Facebook Servers User Phone Numbers». En: *ZDNet*, 29 de junio de 2013. <<

[58] Dylan Love. «It *Looks* like the Facebook Android App Can Control Your Camera and Take Pictures Without Telling You». En: *Business Insider*, 10 de mayo de 2013; Chris Gayomali. «Why Is Facebook's App Asking to Read Your Text Messages?». En: *Fast Company*, 28 de enero de 2014. <<

[59] «Facebook Mobile Update Raises Serious Privacy Concerns». En: *RT*, 3 de diciembre de 2012. <<

[60] Liam Tung. «Microsoft Points Scroogled War Machine at Privacy Worries over Android Apps». En: *ZDNet*, 10 de abril de 2013. <<

[61] Emily Steel y Geoffrey A. Fowler. «Facebook in Privacy Breach». En: *Wall Street Journal*, 8 de octubre de 2010. <<

[62] Kevin J. O’Brien. «Data-Gathering via Apps Presents a Gray Legal Area». En: *New York Times*, 28 de octubre de 2012. <<

[63] Irfan Asrar *et al. Who's Watching You?* McAfee Mobile Security Report, febrero de 2014. <<

[64] McKinsey Global Institute. *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, junio de 2011, pág. 85. <<

[65] Rip Empson. «50M Matches Strong, Hot Mobile Dating App Tinder Is Ready to Go Global, and Move Beyond Flirting». En: *TechCrunch*, 24 de mayo de 2013. <<

[66] Nick Bilton. «Girls Around Me: An App Takes Creepy to a New Level». En: *New York Times*, 30 de marzo de 2012; John Brownlee. «This Creepy App Isn't Just Stalking Women Without Their Knowledge, It's a Wake-Up Call About Facebook Privacy [Update]». En: *Cult of Mac*, 30 de marzo de 2012. <<

[67] Para consultar información adicional, *véase United States v. Jones* (2012), en Wikipedia (versión en inglés), donde se analizan las implicaciones de los datos de ubicación o localización; Junta Editorial. «The Court's GPS Test». En: *New York Times*, 5 de noviembre de 2011. <<

[68] Para consultar un análisis interesante acerca de las implicaciones que tienen para la privacidad los servicios basados en la localización, *véase* el informe de ACLU *Location-Based Services: Time for a Privacy Check-In*. <<

[1] Richard Hartley-Parkinson. «“I’m Going to Destroy America and Dig up Marilyn Monroe”: British Pair Arrested in U. S. on Terror Charges over Twitter Jokes». En: *Mail Online*, 31 de enero de 2012. <<

[2] Kharunya Paramaguru. «Private Data-Collection Firms Get Public Scrutiny». En: *Time*, 19 de diciembre de 2013. <<

[3] Natasha Singer. «Acxiom, the Quiet Giant of Consumer Database *Marketing*». En *New York Times*, 16 de junio de 2012. <<

[4] Eli Pariser. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. Nueva York: Penguin Press, 2012, pág. 43; Natasha Singer. «A Data Broker Offers a Peek Behind the Curtain». En: *New York Times*, 31 de agosto de 2013; Brandon Bailey. «Online Data Brokers Know You-Surprisingly Well». MercuryNews.com, 8 de septiembre de 2013. <<

[5] Alice E. Marwick. «How Your Data Are Being Deeply Mined». En: *New York Review of Books*, 9 de enero de 2014. <<

[6] Lori B. Andrews. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*. Nueva York: Free Press, 2013, pág. 35. <<

[7] Stephanie Armour. «Data Brokers Come Under Fresh Scrutiny: Consumer Profiles Marketed to Lenders». En: *Wall Street Journal*, 12 de febrero de 2014. <<

[8] Paramaguru. «Private Data-Collection Firms Get Public Scrutiny»; «“Data Brokers” Selling Personal Info of Rape Victims to Marketers-Report». En: *RT*, 19 de diciembre de 2013. <<

[9] Matt Pearce. «Dad Gets OfficeMax *Mail* Addressed “Daughter Killed in Car Crash”». En: *Los Angeles Times*, 19 de enero de 2014. <<

[10] Nesita Kwan. «OfficeMax Sends Letter to “Daughter Killed in Car Crash”». NBC Chicago, 19 de enero de 2014. <<

[11] Armour. «Data Brokers Come Under Fresh Scrutiny». <<

[12] Judith Aquino. «Acxiom Prepares New “Audience Operating System” amid Wobbly Earnings». En: *Ad Exchanger*, 1 de agosto de 2013. <<

[13] David Talbot. «A Phone That Knows Where You’re Going». En: *MIT Technology Review*, 9 de julio de 2012. <<

[14] Steve Lohr. «How Privacy Vanishes Online». En: *New York Times*, 16 de marzo de 2010. <<

[15] Carolyn Y. Johnson. «Project “Gaydar”». Boston.com, 20 de septiembre de 2009; Matthew Moore. «Gay Men “Can Be Identified by Their Facebook Friends”». En: *Telegraph*, 21 de septiembre de 2009; Mona Chalabi. «State-Sponsored Homophobia: Mapping Gay Rights Internationally». En: *Guardian*, 10 de marzo de 2014. <<

[16] Emine Saner. «Gay Rights Around the World: The Best and Worst *Countries* for Equality». En: *Guardian*, 30 de julio de 2013. <<

[17] Josh Halliday. «Facebook Users Unwittingly Revealing Intimate Secrets, Study Finds». En: *Guardian,* 11 de marzo de 2013. <<

[18] «Google CEO on Privacy (VIDEO): “If You Have Something You Don’t Want Anyone to Know, Maybe You Shouldn’t Be Doing It”». En: *Huffington Post*, 18 de marzo de 2010. <<

[19] Bobbie Johnson. «Privacy No Longer a Social Norm, Says Facebook Founder». En: *Guardian*, 10 de enero de 2010. <<

[20] «Sharing to the Power of 2012». En: *Economist*, 17 de noviembre de 2011. <<

[21] Moxie Marlinspike. «Why “I Have Nothing to Hide” Is the Wrong Way to Think About Surveillance». En: *Wired*, 13 de julio de 2013. <<

[22] Viktor Mayer-Schönberger y Kenneth Cukier. *Big Data: la revolución de los datos masivos* (traducción de Antonio Iriarte Jurado). Madrid: Turner publicaciones, 2013. <<

[23] Elizabeth A. Harris y Nicole Perlroth. «For Target, the Breach Numbers Grow». En: *New York Times*, 10 de enero de 2014. <<

[24] Geoffrey A. Fowler. «When the Most Personal Secrets Get Outed on Facebook». En: *Wall Street Journal*, 13 de octubre de 2012. <<

[25] Daniel Zwerdling. «Your Digital Trail: Private Company Access». En: *All Tech Considered* (blog), NPR.org, 1 de octubre de 2013. <<

[26] Katie Lobosco. «Facebook Friends Could Change Your Credit Score». En: *CNNMoney*, 27 de agosto de 2013. <<

[27] Viktor Mayer-Schönberger y Kenneth Cukier. *Big Data: la revolución de los datos masivos*. <<

[28] *Véase United States v. Miller*, 425 U. S. 435 (1976), un caso que llegó ante el Tribunal Supremo de Estados Unidos e implicaba la obtención mediante petición judicial de los informes bancarios del señor Miller. Los abogados de Miller argumentaron que el cumplimiento de dicha petición que había realizado la entidad bancaria tenía un alcance irrazonable, el cual infringía los derechos garantizados por la Cuarta Enmienda. En cambio, el tribunal, decidió por seis votos a favor y tres en contra que los documentos obtenidos judicialmente no eran documentos personales de Miller, sino parte de los registros empresariales del banco; por ende, no podía considerarse que los derechos de Miller hubieran sido infringidos cuando una tercera parte (su banco) transmitió al gobierno la información que su cliente le había proporcionado. El legado de Miller nos acompaña en el presente y los defensores de la privacidad han afirmado que la decisión con respecto a Miller carecía de validez a tenor de las técnicas de compartición, producción y almacenamiento que utilizamos en el presente. *Véase* también *Smith v. Maryland*, 442 U. S. 735 (1979), con relación al uso de «grabadores de números marcados» para el seguimiento de todas las llamadas telefónicas realizadas y recibidas. <<

[29] John Stevens. «The Facebook Divorces: Social Network Site Is Cited in “a THIRD of Splits”». En: *Mail Online*, 30 de diciembre de 2011. <<

[30] Mathew Ingram. «Yes, Virginia, HR Execs Check Your Facebook Page». En: *Gigaom*, 27 de enero de 2010; CrossTab. «Online Reputation in a Connected World». Job-hunt.com, enero de 2010. <<

[31] Manuel Valdes. «Job Seekers Getting Asked for Facebook Passwords». En: *Yahoo! Finance*, 20 de marzo de 2012. <<

[32] Jonathan Dame. «Will Employers Still Ask for Facebook Passwords in 2014?». En: *USA Today*, 10 de enero de 2014. <<

[33] «Minnesota Girl Alleges School Privacy Invasion». CNN, 10 de marzo de 2012. <<

[34] Pete Thamel. «Universities Track Athletes Online, Raising Legal Concerns». En: *New York Times*, 30 de marzo de 2012. <<

[35] Asociación Internacional de Jefes de Policía, Resultados del informe sobre las redes sociales de 2013, consultado en Internet el 12 de marzo de 2014, http://www.iacpsocialmedia.org/. <<

[36] Marcia Hoffman. «EFF *Posts* Documents Detailing Law Enforcement Collection of Data from Social Media Sites». Electronic Frontier Foundation, 16 de marzo de 2010. *Véase* también: «IRT-WBT Content 2009», presentación del curso de formación en redes sociales del IRS, 2009, y John Lynch y Jenny Ellickson. «Obtaining and Using Evidence from Social Networking Sites», presentación, Departamento de Justicia de Estados Unidos, División de Delitos, Sección de Delitos Informáticos y Propiedad Intelectual, agosto de 2009. <<

[37] Don Reisinger. «AT&T Reports More Than 300,000 Data Requests in 2013». En: *CNET*, 18 de febrero de 2014. <<

[38] Kim Zetter. «Feds “Pinged” *Sprint* GPS Data 8 Million Times over a Year». En: *Wired*, 1 de diciembre de 2009. <<

[39] Marwick. «How Your Data Are Being Deeply Mined». <<

[40] Charlie Savage. «CIA Is Said to Pay AT&T for Call Data». En: *New York Times*, 7 de noviembre de 2013. <<

[41] «CIA's "Facebook" Program Dramatically Cut Agency's Costs». Onion News Network, consultado el 15 de marzo de 2014. <<

[42] Drew F. Cohen. «It Costs the Government Just 6.5 Cents an Hour to Spy on You». En: *Politico*, 10 de febrero de 2014. <<

[43] Charles Cooper. «Ex-Stasi Boss Green with Envy over NSA's Domestic Spy Powers». En: *CNET*, 28 de junio de 2013. <<

[44] Maria Aspan. «How Sticky Is Membership on Facebook? Just Try Breaking Free». En: *New York Times*, 11 de febrero de 2008; Chamakhe Maurieni. *Facebook Is Deception* (vol. I). WSIC EBooks Ltd., 2012. <<

[1] Associated Press. «Filipino Police Arrest 4 Suspected AT&T *Hackers*». CBS News, 27 de noviembre de 2010; Somini Sengupta. «Phone Hacking Tied to Terrorists». En: *New York Times*, 26 de noviembre de 2011; Marc Goodman. «What Business Can Learn from Organized Crime». En: *Harvard Business Review*, noviembre de 2011. <<

[2] Lauren Indvik. «92% of U. S. Toddlers Have Online Presence». En: *Mashable*, 7 de octubre de 2010. <<

[3] Allegra Tepper. «How Much Data Is Created Every Minute?». En: *Mashable*, 22 de junio de 2012; Kristin Burnham. «Facebook's WhatsApp Buy: 10 Staggering Stats». En: *InformationWeek*, 21 de febrero de 2014. <<

[4] Verlyn Klinkenborg. «Trying to Measure the Amount of Information That Humans Create». En: *New York Times*, 12 de noviembre de 2003. <<

[5] McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, mayo de 2011; ponencia de Kevin Kelly en la edición de 2011 de la conferencia Web 2.0: http://blip.tv/web2expo/web-2-0-expo-sf-2011-kevin-kelly-4980011. <<

[6] Foro Económico Mundial. *Personal Data: The Emergence of a New Asset Class*, enero de 2011 <<

[7] Cory Doctorow. «Personal Data Is as Hot as Nuclear Waste». En: *Guardian*, 15 de enero de 2008. <<

[8] Emma Barnett. «*Hackers* Go After Facebook Sites 600,000 Times Every Day». En: *Telegraph*, 29 de octubre de 2011; Mike Jaccarino. «Facebook *Hack* Attacks Strike 600,000 Times per Day, Security Firm Reports». *Daily News* (edición de Nueva York), 29 de octubre de 2011. <<

[9] «Digital Security Firm Says Most People Use One Password for Multiple Websites». En: *GMA News Online*, 9 de agosto de 2013. <<

[10] «LinkedIn *Hack*», Wikipedia (en inglés); Jose Pagliery. «2 Million Facebook, Gmail, and Twitter Passwords Stolen in Massive *Hack*». En: *CNNMoney*, 4 de diciembre de 2013. <<

[11] Elinor Mills. «Report: Most Data Breaches Tied to Organized Crime». En: *CNET*, 27 de julio de 2010. <<

[12] Jason Kincaid. «Dropbox Security Bug Made Passwords Optional for Four Hours». En: *TechCrunch*, 20 de junio de 2011. <<

[13] John Markoff. «Cyberattack on Google Said to Hit Password System». En: *New York Times*, 19 de abril de 2010; Kim Zetter. «Report: Google *Hackers* Stole Source Code of Global Password System». En: *Wired*, 20 de abril de 2010. <<

[14] John Leyden. «Acxiom Database *Hacker* Jailed for 8 Years». En: *Register*, 23 de febrero de 2006; Damien Scott y Alex Bracetti. «The 11 Worst Online Security Breaches». Complex.com, 9 de mayo de 2012. <<

[15] Brian Krebs. «Experian Sold Customer Data to ID Theft Service». En: *Krebs on Security*, 20 de octubre de 2013. <<

[16] Byron Acohido. «Scammer Dupes Experian into Selling Social Security Nos». En: *USA Today*, 21 de octubre de 2013; Matthew J. Schwartz. «Experian Sold Data to Vietnamese ID Theft *Ring*». En: *Dark Reading*, 21 de octubre de 2013. <<

[17] Jim Finkle y Karen Freifeld. «Exclusive: U. S. States Probing Security Breach at Experian Unit». Reuters, 3 de abril de 2014. <<

[18] Kashmir Hill. «Celebs' Financial Details Leaked, Including Credit Reports for Jay-Z and FBI Director Robert Mueller». En: *Forbes*, 11 de marzo de 2013. <<

[19] Matthew J. Schwartz. «Exposed Website Reboots, Reveals Celeb Credit Reports». En: *InformationWeek*, 4 de abril de 2013. <<

[20] Yasha Levine. «Surveillance Valley Scammers! Why *Hack* Our Data When You Can Just Buy It?». En: *Pando Daily*, 8 de enero de 2014. <<

[21] Graeme McMillan. «40% of Social Network Users Attacked by Malware». En: *Time*, 23 de marzo de 2011. <<

[22] Farooqui Adnan. «MH370 Links on Social Networks Spreading Malware». En: *Ubergizmo*, 18 de marzo de 2014. <<

[23] Riva Richmond. «Koobface Gang That Spread Worm on Facebook Operates in the Open». En: *New York Times*, 16 de enero de 2012. <<

[24] Christopher Williams. «Facebook Versus Russia's Koobface Gang». En: *Telegraph*, 19 de enero de 2012. <<

[25] Joseph L. Flatley. «Firesheep Makes Stealing Your *Cookies*, Accessing Your Facebook Account Laughably Easy». En: *Engadget*, 25 de octubre de 2010; Gary LosHuertos. «Herding Firesheep in Starbucks». En: *CNNMoney*, 16 de diciembre de 2010. <<

[26] Lara Naaman, Jen Pereira y Emily Yacus. «Online Games Can Lead to Identity Theft». ABC News, 16 de julio de 2008. <<

[27] Kristin Finklea. «Identity Theft: Trends and Issues». Servicio de Investigación del Congreso de Estados Unidos, 16 de enero de 2014; Regina Lewis. «Money Quick Tips, Protect Yourself from Identity Theft». En: *USA Today*, 5 de abril de 2014. <<

[28] Blake Ellis. «Identity Fraud Hits New Victim Every Two Seconds». En: *CNNMoney*, 6 de febrero de 2014. <<

[29] Daniel Bortz. «Identity Theft: Why Your Child May Be in Danger». En: *U. S. News & World Report*, 5 de febrero de 2013. <<

[30] RichardPower. «ChildIdentityTheft». Carnegie Mellon CyLab, 2011. <<

[31] Edudemic Staff. «The 21 Best Resources for 2014 to Prevent Cyberbullying». En: *Edudemic*, 17 de octubre de 2014. Para información adicional, *visítese*: http://www.ncpc.org/*cyberbullying*. <<

[32] «*Shock* at Woman's "Facebook Murder"». BBC, 17 de mayo de 2010; Amy Dale Court. «Christopher Dannevig's in Court for Nona Belomesoff Murder After Meeting on a Dating Website, a Court Heard». En: *Daily Telegraph*, 4 de agosto de 2012. <<

[33] «Jealous Lover Flew 4,000 Miles to Stab Ex-Girlfriend to Death after Seeing Her on Facebook with Another Man». En: *Daily Mail*, 10 de marzo de 2010. <<

[34] Raquel Delevi y Robert S. Weisskirch. «Personality Factors as Predictors of Sexting». En: *Computers in Human Behavior* 29 (2013), págs. 2589-2594, con alusión a un estudio realizado por Michelle Drouin y Carly Landgraff. «Texting, Sexting, and Attachment in College Students' Romantic Relationships». En: *Computers in Human Behavior* 28 (2012), págs. 444-449. <<

[35] Sam Biddle. «Here's Where the Naked Pics You Sexted Will End Up». En: *Gizmodo*, 28 de noviembre de 2012. <<

[36] Camille Dodero. «Hunter Moore Makes a Living Screwing You». En: *Village Voice*, 4 de abril de 2012. <<

[37] Mary Madden *et al*. «Teens and Technology 2013». Pew Research Center, 13 de marzo de 2013. <<

[38] McAfee. «McAfee Digital Deception Study 2013: Exploring the Online Disconnect Between Parents & Pre-teens, Teens, and Young Adults», 28 de mayo de 2013. <<

[39] Lancaster University. «*Software* Developers Tackle Child Grooming on the Net». En: *ScienceDaily*, 2 de junio de 2010. <<

[40] Sonia Elks. «Xbox Paedophile Predators “Move in on Prey Within Two Minutes of Contact”». En: *Metro*, 17 de abril de 2012; Bill Singer. «Child Pornography Hid Behind XBox LIVE “Call of Duty: Modern Warfare 2”». En: *Forbes*, 4 de noviembre de 2011. <<

[41] Nicholas Kristof. «He Was Supposed to Take a Photo». En: *New York Times*, 22 de marzo de 2014. <<

[42] Kevin Morris. «BlogTV and the Sad, Avoidable Path to Amanda Todd's Suicide». En: *Daily Dot*, 15 de octubre de 2012. <<

[43] Gillian Shaw. «Amanda Todd’s Mother Speaks Out About Her Daughter, Bullying». En: *Vancouver Sun*, 13 de marzo de 2013. <<

[44] El vídeo está disponible en http://www.youtube.com/watch?v =vOHXGNxE7E. Es profundamente conmovedor y potente y narra la historia de Amanda Todd en sus propias palabras. Un testamento convincente de visionado obligatorio acerca de una vida cercenada demasiado pronto. <<

[45] Patrick McGuire. «The Suspicious Return of the Daily Capper». En: *VICE*, 12 de noviembre de 2012. <<

[46] «Paedophiles Trawl Dating Sites to Get at Kids of Lonely Mums». News.com.au, 12 de diciembre de 2011. <<

[47] David Ferguson. «Texas Teen Viciously Beats and Abducts Gay Man After Targeting Him on Dating Website». En: *Raw Story*, 26 de febrero de 2014. <<

[48] El documental muestra a bandas de justicieros antihomosexuales en Rusia, así como el movimiento religioso antigay que se da en Rusia de manera general. «Gay and Russian: “It’s Hunting Season, We Are the Hunted”». Channel 4 News, 5 de febrero de 2014. <<

[49] Dan Savage. «Anti-gay Russian Neo-Nazis Using Instagram and Facebook to Organize, Publicize Attacks». En: *Stranger*, 11 de febrero de 2014; «Welcome to the Gay-Hating Olympics: Footage of Horrific Beatings Suffered by Gays in Russia». En: *Daily Mail*, 4 de febrero de 2014. <<

[50] Andrew Hough. «Please Rob Me Website Causes Fury for “Telling Burglars When Twitter Users Are Not Home”». En: *Telegraph*, 19 de febrero de 2010. <<

[51] Nick Bilton. «Burglars Said to Have Picked Houses Based on Facebook Updates». En: *Bits* (blog), *New York Times*, 12 de septiembre de 2010. <<

[52] Matt Liebowitz. «Social Media *Status* Updates Tip *Off* Burglars, Study *Shows*». MSNBC, 7 de noviembre de 2011. <<

[53] Gerald Friedland y Robin Sommer. «Cybercasing the Joint: On the Privacy Implications of Geo-*tagging*». International Computer Science Institute y Lawrence Berkeley National Laboratory; «Featured Research: Geo-*tagging*». International Computer Science Institute, acceso realizado el 30 de marzo de 2014; Niraj Chokshi. «How Tech-Savvy Thieves Could "Cybercase" Your House». En: *Atlantic*, 22 de julio 2010. <<

[54] Brendan Keefe. «Exif Data Hiding in Your Photos Targeted by Thieves and Criminal Investigators». YouTube, 5 de noviembre de 2013, http://www.youtube.com/watch?v=mdoD7X8n46Q. <<

[55] Richard Burnett. «Scammers Use Social Networking Info to Target Vacationers' Relatives: Scams Using Social-Networking Vacation». En: *Orlando Sentinel*, 22 de junio de 2013. <<

[56] Robert Beckhusen. «Mexican Cartels Hang, Disembowel “Internet Snitches”». En: *Danger Room* (blog), *Wired*, 15 de septiembre de 2011. <<

[57] Ibíd. <<

[58] Mike Levine. «Officials Warn Facebook and Twitter Increase Police Vulnerability». FoxNews.com, 10 de mayo de 2011. <<

[59] Josh Halliday y Charles Arthur. «Anonymous's Release of Met and FBI Call Puts *Hacker* Group Back Centre Stage». En: *The Guardian*, 2 de febrero de 2012. <<

[60] Bob Christie. «Ariz. Police Confirm 2nd *Hack* on Officers'*Email*». MSNBC.com, 29 de junio de 2011; Mohit Kumar. «77 Law Enforcement Websites Hit in Mass Attack by #Antisec Anonymous». En: *The Hacker News*, 30 de julio de 2011. <<

[61] «Cyber-Criminals Use Facebook to Steal Identity of Interpol Chief». En: *Daily Mail*, 20 de septiembre de 2010. <<

[62] Geoff Nairn. «Your Wall Has Ears». En: *Wall Street Journal*, 19 de octubre de 2011. <<

[63] Michael Riley y Ashlee Vance. «Inside the Chinese *Boom* in Corporate Espionage». En: *BusinessWeek*, 15 de marzo de 2012. <<

[64] Joan Lappin. «American Superconductor and Its Rogue Employee Both Duped by Sinovel». En: *Forbes*, 27 de septiembre de 2011. <<

[65] Carl Sears y Michael Isikoff. «Chinese Firm Paid Insider “to Kill My Company”, American CEO Says». NBCNews.com, 6 de agosto de 2013. <<

[1] «Massive Search for Missing Girl». BBC, 25 de marzo de 2002. <<

[2] «TV Appeal for Missing Amanda». BBC, 28 de marzo de 2002. <<

[3] Nick Davies. «Phone-Hacking Trial Failed to Clear Up Mystery of Milly Dowler's Voicemail». En: *Guardian*, 26 de junio de 2014. <<

[4] «Milly’s *Body* Found». BBC, 21 de septiembre 2002. <<

[5] «Phone Hacking». En: *Guardian*, 7 de febrero de 2011; CNN Library. «UK Phone Hacking Scandal Fast Facts». CNN, 5 de julio de 2014; «News International Phone Hacking Scandal». Wikipedia (en inglés). <<

[6] Nick Davies. «Phone-Hacking Trial Failed to Clear Up Mystery of Milly Dowler's Voicemail». *The Guardian*, 26 de junio de 2014. <<

[7] «Milly Dowler's Phone Was Hacked by News of the World». En: *Telegraph*, 4 de julio de 2011. <<

[8] McAfee. «Mobile Malware in 2014», 25 de marzo de 2014, http://blogs.mcafee.com/; Juniper Networks. «Trusted Mobility Index», mayo de 2012, http:// www.juniper.net/. <<

[9] Cisco. *Cisco 2014 Annual Security Report*; Jordan Kahn. «Apple SVP Phil Schiller Shares Report Showing Android Had 99% of Mobile Malware Last Year». *9to5Google*, 21 de enero de 2014. <<

[10] Rolfe Winkler. «Android Market Share Hits New Record». *Digits* (blog), *Wall Street Journal*, 31 de julio de 2014; Canalys. «Over 1 Billion Android-Based Smart Phones to Ship in 2017», 4 de junio de 2013. <<

[11] Rachel Metz. «Phone Makers' Android Tweaks Cause Security Problems». En: *Technology Review*, 5 de noviembre de 2013; Liam Tung. «What's Making Your Android Insecure? Blame Those Free Apps You Never Asked For». En: *ZDNet*, 6 de noviembre de 2013. <<

[12] Daisuke Wakabayashi. «Cook Raises, Dashes Hopes for Excitement at Apple Annual Meeting». En: *Digits* (blog), *Wall Street Journal*, 28 de febrero de 2014. <<

[13] Juniper Networks. *Juniper Networks Third Annual Mobile Threats Report-March 2012 Through March 2013.* <<

[14] Mike Isaac. «Google Beefs Up Android Market Security». *Wired*, 2 de febrero de 2012. <<

[15] «Report: Malware-Infected Android Apps Spike in the Google *Play* Store». En: *PCWorld*, 19 de febrero de 2014. <<

[16] Joe Krishnan. «Mobile Malware Is Growing and Targeting Android Users, Warn Kaspersky». En: *Independent*, 26 de febrero de 2014; Larry Barrett. «Banking Trojans Emerge as Dominant Mobile Malware Threat». En: *ZDNet*, 24 de febrero de 2014. <<

[17] Brian Krebs. «Mobile Malcoders Pay to (Google) *Play*». En: *Krebs on Security*, 6 de marzo de 2013. <<

[18] Juniper Networks. *Third Annual Mobile Threats Report*, pág. 4. <<

[19] Luke Westaway. «Apple iOS App Store Hit by First Malware App». En: *CNET*, 6 de julio de 2012. <<

[20] Andy Greenberg. «Evasion Is the Most Popular Jailbreak Ever: Nearly Seven Million iOS Devices Hacked in Four Days». En: *Forbes*, 8 de febrero de 2013; Juniper Networks. *Third Annual Mobile Threats Report*. <<

[21] Alice Truong. «This Popular Flashlight App Has Been Secretly Sharing Your Location and Device ID». En: *Fast Company*, 5 de diciembre de 2013; Janel Torkington. «A Flashlight Can Steal from You: How to Stay Safe from Scam Apps». En: *AppsZoom*, 3 de febrero de 2014; Aaron Gingrich. «The Mother of All Android Malware Has Arrived: Stolen Apps Released to the Market That Root Your Phone, Steal Your Data, and Open Backdoor». En: *Android Police*, 6 de marzo de 2011. <<

[22] Juniper Networks. *Third Annual Mobile Threats Report*. <<

[23] Matt Warman. «Fake Android Apps Scam Costs £28,000». En: *Telegraph*, 24 de mayo de 2012. <<

[24] Rich Trenholm. «Android *Spam* Scam Is First Smart Phone Botnet». *CNET*, 6 de julio de 2012. <<

[25] «China Mobile Users Warned About Large Botnet Threat». BBC, 15 enero de 2013; Steven J. Vaughan-Nichols. «First Case of Android Trojan Spreading via Mobile Botnets Discovered». En: *ZDNet*, 5 de septiembre de 2013. <<

[26] «Gartner Says Worldwide PC, Tablet, and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behavior». Gartner Newsroom, 24 de junio de 2013. <<

[27] Salvador Rodriguez. «*Hackers* Can Use Snapchat to Disable iPhones, Researcher Says». En: *Los Angeles Times*, 7 de febrero de 2014. <<

[28] Selena Larson. «Snapchat Responds to Massive *Hack*». En: *ReadWrite*, 3 de enero de 2014. <<

[29] Kashmir Hill. «Snapchats Don’t Disappear: Forensics Firm Has Pulled Dozens of Supposedly Deleted Photos from Android Phones». En: *Forbes*, 9 de mayo de 2013. <<

[30] Tyler Kingkade. «Ohio University Student Accused of Using Nude Snapchat Photos to Extort Sex». En: *Huffington Post*, 30 de diciembre de 2013. <<

[31] Juniper Networks. «Trusted Mobility Index», mayo de 2012. <<

[32] Brian Montopoli. «For Criminals, *Smartphones* Becoming Prime Targets». CBS News, 7 de agosto de 2013; Dan Nosowitz. «A Hacked Mobile Antenna in a Backpack Could Spy on Cell Phone Conversations». En: *Popular Science*, 16 de julio de 2013. <<

[33] «Why Does Kenya Lead the World in Mobile Money?». En: *Economist*, 27 de mayo de 2013. <<

[34] Claire Pénicaud. «State of the Industry: Results from the 2012 Global Mobile Money Adoption Survey». GSMA, febrero de 2013. <<

[35] Keith Wagstaff. «Google Wallet *Hack Shows* NFC Payments Still Aren’t Secure». En: *Time*, 10 de febrero de 2012. <<

[36] Sarah Clark. «Google Wallet Faces Its Second *Hack* of the Week». En: *NFC World*, 10 de febrero de 2012. <<

[37] Anthony Wing Kosner. «Tinder Dating App Users Are Playing with Privacy Fire». En: *Forbes*, 18 de febrero de 2014. <<

[38] Miles Kemp. «Police Warn Photos of Kids with Geo-*tagging* Being Used by Paedophiles». En: *Herald Sun* (Melbourne), 18 de abril de 2012. <<

[39] Shannon Catalano. «Stalking Victims in the United States-Revised». Informe especial del Departamento de Justicia de Estados Unidos, septiembre de 2012; Sean Gallagher. «A Spurned Techie's Revenge: Locking Down His Ex's Digital Life». En: *Ars Technica*, 22 de noviembre de 2013; Justin Scheck. «Stalkers Exploit Cellphone GPS». En: *Wall Street Journal*, 3 de agosto de 2010. <<

[40] Australian Associated Press. «Simon Gittany Jailed for Minimum 18 Years for Murdering Fiancee». En: *Guardian*, 10 de febrero de 2014; Timothy Geigner. «Mobile Spyware Use in Domestic Violence Ramps Up». En: *Wireless News*, 3 de abril de 2014. <<

[41] Scheck. «Stalkers Exploit Cellphone GPS». <<

[42] Ibíd. <<

[43] Quentin Fottrell. «5 Apps for Spying on Your Spouse». En: *Market Watch*, 25 de agosto de 2014. <<

[44] Scheck. «Stalkers Exploit Cellphone GPS». <<

[45] Cheryl Rodewig. «Geotagging Poses Security Risks». Ejército de Estados Unidos, archivo de noticias, 7 de marzo de 2012, www.army.mil. <<

[46] *Ibíd.* <<

[47] El producto puede encontrarse ahora en http://www.trackingkey.com. <<

[48] Para consultar un excelente análisis sobre las implicaciones tanto sociales como para la privacidad de los lectores de matrículas automáticos, *véase* el informe de ls Sindicato por las Libertades Civiles de Estados Unidos *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements* (en inglés). <<

[49] Julia Angwin y Jennifer Valentino-Devries. «New Tracking Frontier: Your License Plates». En: *Wall Street Journal*, 29 de septiembre de 2012. <<

[50] *Ibíd.* <<

[51] Kate Crawford. «San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error». ACLU (blog), 15 de mayo de 2014. <<

[52] Quentin Hardy. «Technology Turns to Tracking People Offline». En: *Bits* (blog), *New York Times*, 7 de marzo de 2013; Gene Marks. «Why the Home Depot Breach Is Worse Than You Think». En: *Forbes*, 22 de septiembre de 2014. <<

[53] Frederic Lardinois. «Google Announces Massive Price Drops for Its Cloud Computing Services and Storage, Introduces Sustained-Use Discounts». En: *Tech Crunch*, 25 de marzo de 2014. <<

[54] Keir Thomas. «Microsoft Cloud Data Breach Heralds Things to Come». En: *PCWorld*, 23 de diciembre de 2010; Ed Bott. «Dropbox Gets Hacked… Again». En: *ZDNet*, 1 de agosto de 2012. <<

[55] Daisuke Wakabayashi y Danny Yadron. «Apple Denies iCloud Breach». En: *Wall Street Journal*, 2 de septiembre de 2014. <<

[56] Jaikumar Vijayan. «Classified Data on President's Helicopter Leaked via P2P, Found on Iranian Computer». En: *Computerworld*, 2 de marzo de 2009. <<

[57] Grupo de Trabajo sobre Amenazas de la Comisión de Ciberseguridad de CSIS. «Threats Posed by the Internet». <<

[58] Dana Priest y William M. Arkin. «A Hidden World, Growing Beyond Control». En: *Washington Post*, 19 de julio de 2010; James Bamford. «The NSA Is Building the *Country*'s Biggest Spy Center (Watch What You Say)». En: *Wired*, 15 de marzo de 2012. <<

[59] Dan Nosowitz. «Every Six Hours, the NSA Gathers as Much Data as Is Stored in the Entire Library of Congress». En: *Popular Science*, 10 de mayo de 2011. <<

[60] Bamford. «NSA Is Building the *Country*'s Biggest Spy Center». <<

[61] Timothy B. Lee. «Here’s Everything We Know About PRISM to Date». En: *Washington Post*, 12 de junio de 2013. <<

[62] James Risen and Laura Poitras. «N. S. A. Gathers Data on Social Connections of U. S. Citizens». En: *New York Times*, 28 de septiembre de 2013. <<

[63] Barton Gellman y Ashkan Soltani. «NSA Collects Millions of *E-mail* Address Books Globally». En: *Washington Post*, 1 de noviembre de 2013. <<

[64] Barton Gellman y Ashkan Soltani. «NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say». En: *Washington Post*, 1 de noviembre de 2013. <<

[65] Floor Boon, Steven Derix y Huib Modderkolk. «NSA Infected 50,000 Computer Networks with Malicious *Software*». En: *Nrc.nl*, 23 de noviembre de 2013. <<

[66] Dustin Volz. «The NSA Is Using Facebook to *Hack* into Your Computer». En: *National Journal*, 12 de marzo de 2014. <<

[67] Spencer Ackerman y James Ball. «Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ». En: *Guardian*, 27 de febrero de 2014. <<

[68] Ashkan Soltani, Rea Petersony Barton Gellman. «NSA Uses Google *Cookies* to Pinpoint Targets for Hacking». En: *Washington Post*, 10 de diciembre de 2013. <<

[69] James Larson, Jeff Glanz y Andrew W. Lehren. «Spy Agencies Tap Data Streaming from Phone Apps». En: *New York Times*, 27 de enero de 2014. <<

[70] Sasha Goldstein. «Angry Birds, Other “Leaky” Cellphone Apps Allow NSA to Collect Massive Amounts of Data: Report». En *Daily News* (edición de Nueva York), 27 de enero de 2014; James Ball. «Angry Birds and “Leaky” Phone Apps Targeted by NSA and GCHQ for User Data». En: *Guardian*, 28 de enero de 2014. <<

[71] Cyrus Farivar. «LOVEINT: On His First Day of Work, NSA Employee Spied on Ex-Girlfriend». En: *Ars Technica*, 27 de septiembre de 2013; Siobhan Gorman. «NSA Officers Spy on Love Interests». En: *Wall Street Journal*, 23 de agosto de 2013. <<

[72] «FinFisher». En: Wikipedia; Vernon Silver. «Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma». En: *Bloomberg*, 25 de julio de 2013. <<

[73] «Syria’s Embattled Dissidents Grapple with Government *Hackers*, Wiretappers, and Impostors». En: *Time*, 1 de junio de 2011; «Social Media: A Double-Edged Sword in Syria». Reuters, 13 de julio de 2011. <<

[74] Andrew E. Kramer. «Ukraine’s Opposition Says Government Stirs Violence». En: *New York Times*, 21 de enero de 2014. <<

[1] Junta de Gobernadores de la OIEA. «Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran», septiembre de 2005. <<

[2] William J. Broad y David E. Sanger. «Report Says Iran Has Data to Make a Nuclear Bomb». En: *New York Times*, 4 de octubre de 2009. <<

[3] David E. Sanger. «Obama Ordered Wave of Cyberattacks Against Iran». En: *New York Times*, 1 de junio de 2012. <<

[4] Marc Ambinder. «Did America's Cyber Attack on Iran Make Us More Vulnerable?». En: *Atlantic*, 5 de junio de 2012. <<

[5] Paul Szoldra. «Blogger Nailsa Major Problem with Facebook's Newsfeed». En: *Business Insider*, 19 de enero de 2014; Jim Tobin. «Facebook Brand Pages Suffer a 44% Decline in Reach since December 1». En: *Ignite Social Media*, 10 de diciembre de 2013. <<

[6] Anthony Wing Kosner. «Watch Out Twitter and Google+, Facebook's News Feed Is Getting Smarter and Smarter». En: *Forbes*, 28 de abril de 2014. <<

[7] Según menciona Eli Pariser en su conferencia TED Talk «Beware Online “Filter Bubbles”», mayo de 2011; René Pickhardt. «What Are the 57 Signals Google Uses to Filter Search Results?», 17 de mayo de 2011, renepickhardt.de. <<

[8] Alex Chitu. «Eric Schmidt on the Future of Search». En: *Google Operating System*, 16 de agosto de 2010. <<

[9] Para consultar un análisis por países sobre la censura mundial en Internet, *véase* OpenNet Initiative en https://opennet.net/about-*filtering*. <<

[10] «Top 10 Internet-Censored *Countries*». En: *USA Today*, 5 de febrero de 2014. <<

[11] Amy Gesenhues. «Survey: 90% of Customers Say Buying Decisions Are Influenced by Online Reviews». Marketingland.com, 9 de abril de 2013; Zendesk. «The Impact of Customer Service on Customer Lifetime Value»; Myles Anderson. «2013 Study: 79% of Consumers Trust Online Reviews as Much as Personal Recommendations». En: *Search Engine Land*, 26 de junio de 2013; Nielsen. *Global Trust in Advertising and Brand Messages*, abril de 2012. <<

[12] Michael Luca. «Reviews, Reputation, and Revenue: The Case of Yelp.com». Documento de trabajo de la Harvard Business School n.º 12-016, septiembre de 2011. <<

[13] Bob Egelko. «Yelp Can Manipulate Ratings, Court Rules». En: *San Francisco Gate*, 4 de septiembre de 2014. <<

[14] Eric Spitznage. «“Operation Clean Turf” and the War on Fake Yelp Reviews». En: *Bloomberg Businessweek*, 25 de septiembre de 2013. <<

[15] Rebecca Grant. «Facebook Has No Idea How Many Fake Accounts It Hasbut It Could Be Nearly 140M». En: *VentureBeat*, 3 de febrero de 2014. <<

[16] Nick Bilton. «Friends, and Influence, for Sale Online». En: *Bits* (blog), *New York Times*, 20 de abril de 2014. <<

[17] John Koetsier. «Facebook's War on Zombie Fans Just Started with a *Boom*». En: *VentureBeat*, 26 de septiembre de 2012. <<

[18] *Ibíd.* <<

[19] Mandi Woodruff. «There Could Be Something Wrong with 42 Million Credit Reports». En: *Business Insider*; Comisión Federal del Comercio, *Informa ante el Congreso*, diciembre de 2012; Melanie Hicken. «Find Out What Big Data Knows About You (It May Be Very Wrong)». En: *CNNMoney*, 5 de septiembre de 2013. <<

[20] Rebecca Smith. «One in Ten Electronic Medical Records Contain Errors: Doctors». En: *Telegraph*, 17 de julio de 2010. <<

[21] «Man Dies During Cancer Drug Trial». BBC, 21 de septiembre de 2008. <<

[22] «California Releases 450 “Violent and Dangerous” Criminals After Computer Glitch Sets Them Free». En: *Daily Mail Online*, 27 de mayo de 2011. <<

[23] «Are You One of the 20,000 People Wrongly Branded a Criminal? Police Blunders Give Thousands Records for Crimes They Have Not Committed». En: *Daily Mail Online*, 28 de diciembre de 2012. <<

[24] Asher Moses. «*Hackers* Break Into Police Computer as Sting Backfires». En: *Sydney Morning Herald*, 18 de agosto de 2009; «*Hacker* "Steals" Hertfordshire Police Officers' Data». BBC News, 30 de agosto de 2012; Sabari Selvan. «Italy's Police Website Vitrociset.it Hacked by #Antisec». En: *E Hacking News*, 30 de julio de 2011; «Ten Months Later, Memphis Police Dept. First Notifies People of Data Breach?». En: *Office of Inadequate Security*, 21 de febrero de 2014; «Montreal Police Database Hacked; Personal Information Posted Online». En: *Global News*, 19 de febrero de 2013; IPCC. «Hacking into Police Force Systems». En: *Learning the Lessons*, mayo de 2013; Jeff Goldman. «Honolulu Police Department Hacked». En: *eSecurity Planet*, 8 de mayo de 2013. <<

[25] «Danish Police Driving Licence Database Hacked by a Top Rated Swedish *Hacker*». En: *Scandinavia Today*, 6 de junio de 2013. <<

[26] «Philadelphia Police Witness Information Hacked». Lawofficer.com, acceso realizado el 9 de noviembre de 2013. <<

[27] «Ex-con Returns to Jail for Hacking Prison Computers». En: *PCWorld*, 15 de noviembre de 2008. <<

[28] David Schultz. «As Patients' Records Go Digital, Theft and Hacking Problems Grow». En: *Kaiser Health News*, 3 de junio de 2012; Kim Zetter. «It's Insanely Easy to *Hack* Hospital Equipment». En: *Wired*, 25 de abril de 2014; Kelly Jackson Higgins. «Anatomy of an Electronic Health Record Zero-Day». En: *Dark Reading*, 4 de diciembre de 2013. <<

[29] Neal Ungerleider. «Medical Cybercrime: The Next Frontier». En: *Fast Company*, 15 de agosto de 2012. <<

[30] Nelson Harvey. «Hospital Database Hacked, Patient Info Vulnerable». En: *Aspen Daily News*, 15 de marzo de 2014. <<

[31] «Victim of Botched Transplant Declared Dead». CNN, 23 de febrero de 2003. <<

[32] EMC Corporation. «2013: A Year in Review», enero de 2014. <<

[33] *Ibíd.* <<

[34] Miles Date. «Why We Need to Support DMARC and Fight Phishing». En: *Deliverability Next*, 2 de abril de 2013. <<

[35] Cisco. *Email Attacks: This Time It's Personal*, junio de 2011. <<

[36] Ben Elgin, Dune Lawrence y Michael Riley. «Coke Gets Hacked and Doesn’t Tell Anyone». En: *Bloomberg*, 4 de noviembre de 2012. <<

[37] Equipo de investigación de TrendLabs APT. «Spear-Phishing *Email*: Most Favored APT Attack Bait». Documento de investigación de Trend Micro Incorporated, 2012. <<

[38] Rob Waugh. «New PC Virus Doesn’t Just Steal Your Money-It Creates Fake Online Bank Statements So You Even Don’t Know It’s Gone». En: *Daily Mail Online*, 6 de enero de 2012. <<

[39] Amy Klein. «Holiday Shopping and Fraud Schemes». En: *Security Intelligence*, 4 de enero de 2012. <<

[40] Carol Todd. «Arrest of Dutch Man in Amanda Todd Cyberbullying Rekindles Family Anguish». CBC News, 28 de abril de 2014. <<

[41] Associated Press. «Netherlands Arrest in Amanda Todd Webcam Blackmail Case». En: *Guardian*, 17 de abril de 2014. <<

[42] Associated Press. «Dutch Man Arrested in Connection with Suicide of Canadian Teen Amanda Todd». En *Daily News* (edición de Nueva York), 18 de abril de 2014. <<

[43] Dan Goodin. «Woman Charged with Cyberbullying Teen on Craigslist». En: *Register*, 18 de agosto de 2009. <<

[44] Corey Grice y Scott Ard. «Hoax Briefly Shaves $2.5 Billion *off* Emulex's Market Cap». En: *CNET*; Jane C. Chesterman. «The Emulex *Stock* Hoax: Potential Liability for Internet Wire and Bloomberg?». En: *Journal of Corporation Law* 27, n.º 1 (otoño de 2001). <<

[45] Securities and Exchange Commission de Estados Unidos. «Defendant in Emulex Hoax Sentenced», 8 de agosto de 2001. <<

[46] Corey Grice. «23-Year-Old Arrested in Emulex Hoax». En: *CNET*, 31 de agosto de 2000. <<

[47] Alex Berenson. «Guilty Plea Is Set in Internet Hoax Case Involving Emulex». En: *New York Times*, 29 de diciembre de 2000. <<

[48] Lina Saigol. «The Murky World of Traders' Electronic Chat». En: *Financial Times*, 11 de noviembre de 2013. <<

[49] «FBI Arrests Seven in $140 Million Penny *Stock* Fraud». En: *Moneynews*, 14 de agosto de 2013. <<

[50] Amy Chozick. «Bloomberg Admits Terminal Snooping». En: *New York Times*, 13 de mayo de 2013. <<

[51] Julia La Roche. «Bloomberg Spying Scandal Escalates». En: *Business Insider*, 10 de mayo de 2013. <<

[52] Mark DeCambre. «Goldman Outs Bloomberg Snoops». En: *New York Post*, 10 de mayo de 2013. <<

[53] Chozick. «Bloomberg Admits Terminal Snooping». <<

[54] Michael Lewis. «An Adaptation from "*Flash* Boys: A Wall Street Revolt" by Michael Lewis». En: *New York Times*, 31 de marzo de 2014. <<

[1] Kelly Jackson Higgins. «“Robin Sage” Profile Duped Military Intelligence, IT Security Pros». En: *Dark Reading*, 6 de julio de 2010. <<

[2] Thomas Ryan. «Getting in Bed with Robin Sage». Provide Security, 2010; Shaun Waterman «Fictitious Femme Fatale Fooled Cybersecurity». En: *Washington Times*, 18 de julio de 2010. <<

[3] Robert McMillan. «Paris Hilton Accused of Voice-*Mail* Hacking». En: *InfoWorld*, 25 de agosto de 2006. <<

[4] Ron Lieber. «Your Voice *Mail* May Be Even Less Secure Than You Thought». En: *New York Times*, 19 de agosto de 2011. <<

[5] Byron Acohido. «Caller ID Spoofing Scams Aim for Bank Accounts». En: *USA Today*, 15 de marzo de 2012. <<

[6] Kathy Kristof. «IRS Warns of Biggest Tax Scam Ever». En: *MoneyWatch*, 20 de marzo de 2014. <<

[7] Adrianne Jeffries. «Meet “Swatting”, the Dangerous Prank That Could Get Someone Killed». En: *Verge*, 23 de abril de 2013. <<

[8] Maria Elena Fernandez. «Ashton Kutcher, Miley Cyrus & Others Terrorized in Dangerous “Swatting” Prank». En: *Daily Beast*, 5 de octubre de 2012. <<

[9] FBI. «The Crime of “Swatting”: Fake 9-1-1 Calls Have Real Consequences», acceso realizado el 7 de mayo de 2014. <<

[10] Alan Duke. «Boy Admits “Swatting” Ashton Kutcher, Justin Bieber». CNN, 12 de marzo de 2013. <<

[11] Heidi Fenton. «Swatting-Related Crash». Mlive.com, 8 de abril de 2014. <<

[12] Sebastian Anthony. «The Secret Second Operating System That Could Make Every Mobile Phone Insecure». En: *ExtremeTech*, 13 de noviembre de 2013. <<

[13] Ralf Philipp Weinmann. «DeepSec 2010: All Your Baseband Are Belong to Us». YouTube, http://www.youtube.com/watch?v=fQqv0v14KKY, acceso realizado el 7 de mayo de 2014. <<

[14] Paul K. «Replicant Developers Find and Close Samsung Galaxy Backdoor». Free *Software* Foundation, 12 de marzo de 2014. <<

[15] Declan McCullagh. «FBI Taps Cell Phone Mic as Eavesdropping Tool». En: *ZDNet*, 1 de diciembre de 2006. <<

[16] Hard Reg. «Driver Follows Satnav to His Doom». En: *Register*, 5 de octubre de 2010. <<

[17] Departamento de Seguridad Nacional de Estados Unidos. «National Risk Estimate», 9 de noviembre de 2011. <<

[18] Robert Charette. «Are We Getting Overly Reliant on GPS-Intensive Systems?». IEEE Spectrum, 9 de marzo de 2011, disponible en spectrum.ieee.org. <<

[19] David Hambling. «GPS Chaos: How a $30 Box Can Jam Your Life». En: *New Scientist*, 6 de marzo de 2011. <<

[20] «Out of Sight». En: *Economist*, 27 de julio de 2013. <<

[21] John Brandon. «GPS Jammers Illegal, Dangerous, and Very Easy to Buy». FoxNews.com, 17 de marzo de 2010. <<

[22] «Out of Sight». <<

[23] Hambling. «GPS Chaos». <<

[24] Charles Arthur. «Car Thieves Using GPS “Jammers”». En: *Guardian*, 22 de febrero de 2010; Matt Warman. «Organised Crime “Routinely Jamming GPS”». En: *Telegraph*, 22 de febrero de 2012; «£6M Lorry Hijackings Gang Face Ten Years». En: *Express & Star*, 6 de mayo de 2010. <<

[25] «The $30 GPS Jammer That Could Paralyze U. S. Cities». En: *Week*, 10 de marzo de 2011. <<

[26] Jeff Coffed. «The Threat of GPS Jamming». Exelis, febrero de 2014. <<

[27] Tom Simonite. «Ship Tracking *Hack* Makes Tankers Vanish from View». En: *MIT Technology Review*, 18 de octubre de 2013. <<

[28] «Researchers *Show* How a Major GPS Flaw Could Allow Terrorists and *Hackers* to Hijack Commercial Ships and Planes». En: *Mail Online*, 27 de julio de 2013; Aviva Hope Rutkin. «"Spoofers" Use Fake GPS Signals to Knock a Yacht *Off* Course». En: *MIT Technology Review*, 14 de agosto de 2013. <<

[29] Sandra Zaragoza. «Spoofing Superyacht at Sea». En: *Know*, 31 de julio de 2013. <<

[30] Kelsey D. Atherton. «Israeli Students Spoof Waze App with Fake Traffic Jam». En: *Popular Science*, 31 de marzo de 2014. <<

[31] Nathan Hodge y Adam Entous. «Oil Firms Hit by *Hackers* from China, Report Says». En: *Wall Street Journal*, 10 de febrero de 2011. <<

[32] Nicole Perlroth. «*Hackers* Lurking in Vents and Soda Machines». En: *New York Times*, 7 de abril de 2014. <<

[33] Hodge y Entous. «Oil Firms Hit by *Hackers* from China». <<

[34] Lee Moran. «Montana Residents Flip Out When Emergency Alert System Tells Them the Zombie Apocalypse Is Happening-Like Right Friggin Now». En *Daily News* (edición de Nueva York), 12 de febrero de 2013. <<

[35] «Russian *Hackers* Jam Automobile Traffic with Porn». Fox News, Tecnología, 15 de enero de 2010; «Russian Jailed for Six Years for Hacking into Advertising Server and Making Electronic Billboard *Show* Porn to Motorists». En: *Mail Online*, 24 de marzo de 2011. <<

[36] Sevil Omer. «Racial Slur on Mich. Road Sign Targets Trayvon Martin». NBC News, 9 de abril de 2012 <<

[37] Serge Malenkovich. «Hacking the Airport Security Scanner». En: *Kaspersky Lab*. 14 de marzo de 2014. <<

[38] «Hacked X-Rays Could Make TSA Scanners Useless», vídeo. En: *Wall Street Journal*, 12 de febrero de 2014. <<

[39] Kim Zetter. «Hacked X-Rays Could *Slip* Guns Past Airport Security». En: *Wired*, 11 de febrero de 2014. <<

[40] Departamento de Transporte de Estados Unidos. «Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems». ID de proyecto: FI-2009-049, 4 de mayo de 2009. <<

[41] «FAA’s Air-Traffic Networks Breached by *Hackers*». En: *Wall Street Journal*, 7 de mayo de 2009. <<

[42] Thomas Claburn. «Air Traffic Control System Repeatedly Hacked». En: *Dark Reading*, 7 de mayo de 2009. <<

[43] Steve Henn. «Could the New Air Traffic Control System Be Hacked?». NPR. org, 14 de agosto de 2012. <<

[44] Donald McCallie, Jonathan Butts y Robert Mills. «Security Analysis of the ADS-B Implementation in the Next Generation Air Transportation System». En: *International Journal of Critical Infrastructure Protection* 4, n.º 2 (agosto de 2011), págs. 78-87, doi:10.1016/ j.ijcip.2011.06.001. <<

[45] «The World of 100% Election Victories». BBC News, 11 de marzo de 2014. <<

[46] «Hacking the Vote: Internet Systems Remain Unsecure». CNN, 5 de noviembre de 2012. <<

[47] Andrew Tarantola. «Hacked DC School Board E-*voting* Elects Bender President». En: *Gizmodo*, 2 de marzo de 2012. <<

[48] Walter L. Sharp. «Electronic Warfare». Joint Publication 3-13.1, 26 de enero de 2007 <<

[49] Adam Martin. «Reuters Blogs Hacked with Fake Story About Syrian Rebel Retreat». En: *Wire*, 3 de agosto de 2012. <<

[50] Erich Follath y Holger Stark. «The Story of “Operation Orchard”: How Israel Destroyed Syria’s Al Kibar Nuclear Reactor». En: *Spiegel Online*, 11 de febrero de 2009; David E. Sanger y Mark Mazzetti. «Israel Struck Syrian Nuclear Project, Analysts Say». En: *New York Times*, 14 de octubre de 2007. <<

[51] Lewis Page. «Israeli Sky-*Hack* Switched *off* Syrian Radars Countrywide». En: *Register*, 22 de noviembre de 2007. <<

[52] Yuval Goren. «IDF Reserve Troops Receive Fictitious Calls for Duty in Gaza». Haaretz.com, 8 de enero de 2009. <<

[53] Balousha Hazem. «Text Messages and Phone Calls Add Psychological Aspect to Warfare in Gaza». En: *Guardian*, 2 de enero de 2009. <<

[54] Nick Fielding e Ian Cobain. «Revealed: US Spy Operation That Manipulates Social Media». En: *Guardian*, 17 de marzo de 2011. <<

[55] *Ibíd.* <<

[56] *Ibíd.* <<

[57] Freedom on the Net 2013, FreedomHouse.org, 3 de octubre de 2013. <<

[58] Serguéi Chérnov. «Internet Troll Operation Uncovered in St. Petersburg». En: *St. Petersburg Times*, 18 de septiembre de 2013. <<

[59] Paul Roderick Gregory. «Inside Putin's Campaign of Social Media Trolling and Faked Ukrainian Crimes». En: *Forbes*, 11 de mayo de 2014. <<

[60] Chris Elliott. «The Readers' Editor on… Pro-Russia Trolling Below the Line on Ukraine Stories». En: *Guardian*, 4 de mayo de 2014; Alec Luhn. «Pro-Kremlin Journalists Secretly Given Awards by Putin». En: *Irish Times*, 9 de mayo de 2014. <<

[61] Katie Hunt y Cy Xu «China “Employs 2 Million to Police Internet”». CNN, 7 de octubre de 2013. <<

[62] Steven Millward. «China Plans Weibo Propaganda Blitz Using 2 Million Paid Commenters». En: *Tech in Asia*, 18 de enero de 2013. <<

[63] John Kennedy. «Beijing Orders Its 2.06 Million “Propaganda Workers” to Get Microblogging». En: *South China Morning Post*, 18 de enero de 2013. <<

[64] Benjamin Carlson. «Party Trolls: Meet China's Answer to the Internet». En: *Global Post*, 28 de enero de 2013. <<

[65] LWG Consulting. «Sites Affected by the Heartbleed Bug», 4 de abril de 2014. <<

[66] Arik Hesseldahl. «Heartbleed Flaw Lurks in Android Apps Downloaded by Millions». En: *Re/code*, 23 de abril de 2014. <<

[67] Mark Prigg. «Over 300,000 Web Sites STILL at Risk from Heartbleed Bug». En: *Mail Online*, 9 de mayo de 2014. <<

[68] Michael Riley. «NSA Said to Exploit Heartbleed Bug for Intelligence for Years». En: *Bloomberg*, 11 de abril de 2014. <<

[69] Hiawatha Bray. «Heartbleed Hoodlums Try to Cash in on Internet Security Bug». En: *Boston Globe*, 18 de abril de 2014; Mark Clayton. «“Heartbleed” Mystery: Did Criminals Take Advantage of Cyber-Security Bug?». En: *Christian Science Monitor*, 9 de abril de 2014. <<

[1] Los detalles del funcionamiento interno de Innovative *Marketing* están extraídos de numerosas fuentes de investigación. La mayor parte de los datos fueron desvelados por Dirk Kollberg, un investigador de McAfee con sede en Hamburgo, Alemania, que invirtió meses en estudiar la empresa. Otros datos adicionales aparecieron en: David Talbot. «The Perfect Scam». En: *MIT Technology Review*, 21 de junio de 2011; Jim Finkle. «Inside a Global Cybercrime *Ring*». Reuters, 24 de marzo de 2010; Comisión Federal de Comercio de Estados Unidos. «Innovative *Marketing*, Inc., *et. al*». 28 de febrero de 2014; Toralv Dirro. «Malicious World». McAfee Labs; Interpol. «Sundin, Björn Daniel»; *United States of America v. Bjorn Daniel Sundin, Shaileshkumar P. Jain, a.k.a. «Sam Jain», and James Reno*, Northern District of Illinois Eastern Division, marzo de 2010; Misha Glenny. «Cybercrime: Is It Out of Control?». En: *Guardian*, 21 de septiembre de 2011; Misha Glenny. «Inside the World of Cybercrime, EIBF 2012, Review». EdinburghGuide.com, 20 de agosto de 2012; Felix Richter. «Twitter's Ad Revenue Tipped to Double This Year». En: *Statista*, 13 de septiembre de 2012; David Talbot. «The Perfect Scam». En: *Technology Review*, 21 de junio de 2011. <<

[2] Oficina de la Naciones Unidas contra la Droga y el Delito. «Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes», octubre de 2011, pág. 7. <<

[3] Misha Glenny. *McMafia: el crimen sin fronteras* (traducción de Joan Trujillo Parra). Barcelona: Destino, 2008. <<

[4] Allison Davis, Patrick Di Justo y Adam Rogers. «Crime, Organized». En: *Wired*, febrero de 2011, pág. 78; General OneFile, web, 22 de mayo de 2014. <<

[5] «Organised Crime in the Digital Age», estudio conjunto de Detica/BAE Systems y el John Grieve Centre for Policing de la London Metropolitan University, marzo de 2012. <<

[6] Lillian Ablon, Martin C. Libicki y Andrea A. Golay. «Markets for Cybercrime Tools and Stolen Data». Rand Corporation, pág. 4. <<

[7] Byron Acohido. «How Kidnappers, Assassins Utilize *Smartphones*, Google, and Facebook». USAToday.com, 18 de febrero de 2011. <<

[8] «Woman “Ran Text-a-Getaway” Service». BBC News, 16 de julio de 2013. <<

[9] Basado en las observaciones personales del autor… y tengo una fotografía que lo atestigua. <<

[10] Dana Sauchelli y Bruce Golding. «Hookers Turning Airbnb Apartments into Brothels». En: *New York Post*, 14 de abril de 2014. <<

[11] La información acerca de la estructuración de las organizaciones de ciberdelincuencia modernas está extraída de múltiples fuentes, incluida mi experiencia e investigaciones personales, consultas con altos cargos de los cuerpos de seguridad que trabajan en el ámbito de la ciberdelincuencia y recursos en Internet como: «Cybercriminals Today Mirror Legitimate Business Processes», Fortinet 2013 Cybercrime Report; Trend Micro Threat Research, «A Cybercrime Hub», agosto de 2009; Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud*, informe conjunto, 6 de abril de 2010; Patrick Thibodeau. «FBI Lists Top 10 *Posts* in Cybercriminal Operations». En: *Computerworld*, 23 de marzo de 2010; Roderic Broadhurst *et al*. «Organizations and Cybercrime». En: *International Journal of Cyber Criminology*, 11 de octubre de 2013. <<

[12] Dimitri Samosseiko. «The Partnerka» (documento presentado en la Conferencia Virus Bulletin, septiembre de 2009); «The Business of Cybercrime». Trend Micro White Paper, enero de 2010. <<

[13] Cisco. *Cisco 2010 Annual Security Report*, pág. 9. <<

[14] Broadhurst *et al*. «Organizations and Cybercrime». <<

[15] Dunn. «Global Cybercrime Dominated by 50 Core Groups». <<

[16] *Véase* Brian Krebs. «“Citadel” Trojan Touts Trouble-*Ticket* System». En: *Krebs on Security*, 23 de enero de 2012. <<

[17] Bob Sullivan. «160 Million Credit Cards Later, “Cutting Edge” Hacking *Ring* Cracked». NBC News, 25 de julio de 2013; «Team of International Criminals Charged with Multimillion Dollar Hacking *Ring*». NBC News, 25 de julio de 2013. <<

[18] Thomas Holt. «Exploring the Social Organisation and Structure of Stolen Data Markets». En: *Global Crime* 14, n.º 2-3 (2013); Thomas Holt. «Honor Among (Credit Card) Thieves?». En: *Michigan State University Today*, 22 de abril de 2013. <<

[19] Ablon, Libicki y Golay. «Markets for Cybercrime Tools and Stolen Data», pág. 17. <<

[20] Gregory J. Millman. «Cybercriminals Work in a Sophisticated Market Structure». En: *Wall Street Journal*, 27 de junio de 2013. <<

[21] Kevin Poulsen. «Superhacker Max Butler Pleads Guilty». En: *Wired*, 29 de junio de 2009. <<

[22] Donald T. Hutcherson. «Crime Pays: The Connection Between Time in Prison and Future Criminal Earnings». En: *Prison Journal* 92, n.º 3 (septiembre de 2012), págs. 315-335; Shankar Vedantam. «When Crime Pays: Prison Can Teach Some to Be Better Criminals», NPR, 1 de febrero de 2013. <<

[23] Ian Gallagher. «Public Schoolboy *Hacker* Who Masterminded £15M Fraud Is Put in Jail's IT Class… and *Hacks* the Prison's Computer System». En: *Mail Online*, 2 de marzo de 2013. <<

[24] Reuters. «San Quentin Prison Becomes an Incubator for Startups». En: *Huffington Post*, 25 de febrero de 2013. <<

[25] Russell Eisenman. «Creativity and Crime: How Criminals Use Creativity to Succeed». En: *The Dark Side of Creativity*, David H. Cropley (ed.) *et al*. Nueva York: Cambridge University Press, 2010. <<

[26] John Leyden. «Malware Devs Embrace Open-Source». En: *Register*, 10 de febrero de 2012. <<

[27] Ablon, Libicki y Golay. «Markets for Cybercrime Tools and Stolen Data», pág. 11. <<

[28] Chris Anderson. *La economía Long-Tail: de los mercados de masas al triunfo de lo minoritario*. Barcelona: Urano, 2009; Goodman. «What Business Can Learn from Organized Crime». <<

[29] Riva Richmond. «Web Site Ranks *Hacks* and Bestows Bragging Rights». En: *New York Times*, 21 de agosto de 2011. <<

[30] Jim Finkle. «Inside a Global Cybercrime *Ring*». Reuters, 24 de marzo de 2010. <<

[31] Paul Peachey. «Cybercrime Boss Offers a Ferrari for *Hacker* Who Dreams Up the Biggest Scam». En: *Independent*, 11 de mayo de 2014. <<

[32] Jeff Howe. «The Rise of Crowdsourcing». En: *Wired*, junio de 2006. <<

[33] Marc Goodman. «The Rise of Crime-Sourcing». En: *Forbes*, 3 de octubre de 2011. <<

[34] *Ibíd.* <<

[35] Elizabeth Fiedler. «Retailers Fight "*Flash* Robs"». NPR.org, 25 de noviembre de 2011; Annie Vaughan. «Teenage *Flash* Mob Robberies on the Rise». FoxNews.com, 18 de junio de 2011. <<

[36] Chris Foresman. «Senator to Apple, Google: Why Are DUI Checkpoint Apps Still Available?». En: *Ars Technica*, 20 de mayo de 2011; «Want to Avoid a Speed Trap or a DUI Checkpoint? There's an App for That». En: *Mail Online*, 21 de marzo de 2011. <<

[37] Patrick Kingsley. «Inside the Anti-*kettling* HQ». En: *Guardian*, 2 de febrero de 2011. <<

[38] «LulzSec Opens *Hack* Request Line». BBC, 15 de junio de 2011. <<

[39] «LulzSec *Hackers* Sets Up Hotline for Attacks». Reuters, 15 de junio de 2011. <<

[40] Brian Krebs. «Wash. Hospital Hit by $1.03 Million Cyberheist». *Krebs on Security*, 30 de abril de 2013. <<

[41] Mathew J. Schwartz. «*Hackers* Offer Free Porn to Beat Security Checks». En: *Dark Reading*, 20 de junio de 2012. <<

[42] Caroline McCarthy. «Bank Robber Hires Decoys on Craigslist, Fools Cop». En: *CNET*, 3 de octubre de 2008. <<

[43] David Pescovitz. «Bank Robber Uses Craigslist to Hire Unsuspecting Accomplices». En: *Boing Boing*, 1 de octubre de 2008; «Armored Truck Robber Uses Craigslist to Make Getaway». King5.com, 21 de septiembre de 2009. <<

[44] Kickstarter, «Stats», acceso realizado el 25 de mayo de 2014, https://www.kickstarter.com/help/stats; se indicaba que Kickstarter había recaudado 1.131.653 de dólares desde su lanzamiento. <<

[45] Jason Del Rey. «Kickstarter Says It Was Hacked (Updated)». En: *Re/code*, 15 de febrero de 2014. <<

[46] «Apple Fingerprint ID “Hacked”». BBC News, 23 de septiembre de 2013. <<

[47] John Bowman, «iPhone 5S Fingerprint Hacking Contest Offers $20K Bounty». En: *Your Community* (blog). CBC News, 20 de septiembre de 2013. <<

[48] Frank. «Chaos Computer Club Breaks Apple TouchID». Chaos Computer Club, 21 de septiembre de 2013. <<

[49] Andy Greenberg. «Meet the “Assassination Market” Creator Who’s Crowdfunding Murder with Bitcoins». En: *Forbes*, 18 de noviembre de 2013. <<

[50] Marc Santora. «In Hours, Thieves Took $45 Million in A. T. M. Scheme». En: *New York Times*, 9 de mayo de 2013. <<

[1] Ken Klippenstein «Dread Pirate Roberts 2.0: An Interview with Silk Road's New Boss». En: *Ars Technica,* 5 de febrero de 2014. <<

[2] Patrick Howell O’Neill. «The Rise and Fall of Silk Road’s Heroin Kingpin». En: *The Daily Dot*, 9 de octubre de 2013. <<

[3] David Segal. «Eagle Scout. Idealist. Drug Trafficker?». En: *New York Times*, 18 de enero de 2014; Kevin Goodman. «The Dark Net». En: *Huffington Post*, 16 de octubre de 2013; Adrian Chen. «The Underground Website Where You Can Buy Any Drug Imaginable». En: *Gawker*, 1 de junio de 2011; Stuart Pfeifer, Shan Li y Walter Hamilton. «End of Silk Road for Drug Users as FBI Shuts Down Website». En: *Los Angeles Times*, 2 de octubre de 2013; Gerry Smith. «Alleged Silk Road Founder Put Out Hit on 6 Enemies, Prosecutors Say». En: *Huffington Post*, 22 de noviembre 2013; Kim Zetter. «Feds Arrest Alleged "Dread Pirate Roberts", the Brain Behind the Silk Road Drug Site». En: *Wired*, 2 de octubre de 2013. <<

[4] Para información adicional acerca de Tor, *visítese* Tor Project en https://www.torproject.org/. <<

[5] Alex Biryukov, Ivan Pustogarov y Ralf-Philipp Weinmann. «Content and Popularity Analysis of Tor Hidden Services». Universidad de Luxemburgo. <<

[6] Geoffrey A. Fowler. «Tor: An Anonymous, and Controversial, Way to WebSurf». En: *Wall Street Journal*, 18 de diciembre de 2012. <<

[7] Raphael Cohen-Almagor. «In Internet's Way». En: *International Journal of Cyber Warfare and Terrorism* 2, n.º 3 (julio-septiembre de 2012), págs. 39-58. <<

[8] Kimberly Dozier. «Virtually Every Terrorist Group in the World Shifting Tactics in Wake of NSA Leaks: U. S. Officials». En: *National Post*, 26 de junio de 2013. <<

[9] «Al Qaeda, Terrorists Changing Communication Methods After NSA Leaks, US Officials Say». Fox News, 26 de junio de 2013; http://www.youtube.com/watch?v=D8Mgpm1PgF4. <<

[10] Michael K. Bergman. «White Paper: The Deep Web: Surfacing Hidden Value». En: *Journal of Electronic Publishing* 7, n.º 1 (agosto de 2001). <<

[11] Steve Lawrence y C. Lee Giles. «Accessibility of Information on the Web». En: *Nature*, 8 de julio de 1999, pág. 107, doi:10.1038/21987. <<

[12] Bergman. «White Paper». <<

[13] Jose Pagliery. «The Deep Web You Don’t Know About». En: *CNNMoney*, 10 de marzo de 2014. <<

[14] «Google Search vs. Deep Web Harvesting». En: *BrightPlanet*, 31 de julio de 2013. <<

[15] Andy Greenberg. «Inside the “Dark Market” Prototype, a Silk Road the FBI Can Never Seize». En: *Wired*, 24 de abril de 2014. <<

[16] Kim Zetter. «New “Google” for the Dark Web Makes Buying Dope and Guns Easy». En: *Wired*, 17 de abril de 2014. <<

[17] Michael Riley. «Stolen Credit Cards Go for $3.50 at Amazon-Like Online Bazaar». En: *Bloomberg*, 19 de diciembre de 2011. <<

[18] Ernesto, 18 de mayo de 2008, blog en *TorrentFreak*, acceso realizado el 27 de junio de 2014. <<

[19] «Inside the Mansion-and Mind-of Kim Dotcom, the Most Wanted Man on the Net». En: *Wired*, 18 de octubre de 2012. <<

[20] Beth Stebner. «The Most Dangerous Drug in the World: “Devil’s Breath” Chemical from Colombia Can Block Free Will, Wipe Memory, and Even Kill». En: *Mail Online*, 12 de mayo de 2012. <<

[21] Forward-Looking Threat Research Team. «Deepweb and Cybercrime». Trend Micro, 2013, pág. 16. <<

[22] Brian Krebs. «Peek Inside a Professional Carding Shop». En: *Krebs on Security*, 4 de junio de 2014. <<

[23] Max Goncharov. «Russian Underground Revisited». Forward-Looking Threat Research Team, Trend Micro Research Paper. <<

[24] Brian Krebs. «Cards Stolen in Target Breach Flood Underground Markets». En: *Krebs on Security*, 20 de diciembre de 2013; Dancho Danchev. «Exposing the Market for Stolen Credit Cards Data». En: *Dancho Danchev's Blog*, 31 de octubre de 2011; «Meet the *Hackers*». En: *Bloomberg Businessweek*, 28 de mayo de 2006; David S. Wall. «The Organization of Cybercrime in an EverChanging Cyberthreat Landscape» (borrador de ponencia para la Criminal Networks Conference, Montreal, 3-4 de octubre de 2011). <<

[25] «Skimming *off* the Top». En: *Economist*, 15 de febrero de 2014. <<

[26] Pew Research Center. «More Online Americans Say They’ve Experienced a Personal Data Breach», 14 de abril de 2014; Rosie Murray-West. «UK Worst in Europe for Identity Fraud». En: *Telegraph*, 1 de octubre de 2012. <<

[27] Herb Weisbaum. «U. S. Health Care System Has $5.6 Billion Security Problem». NBC News, 12 de marzo de 2014; Richard Rubin. «IRS May Lose $21 Billion in Identity Fraud, Study Says». En: *Bloomberg*, 2 de agosto de 2012. <<

[28] «Cashing In on Digital Information». TrendMicro/TrendLabs 2013 Annual Security Roundup. <<

[29] Sam Biddle. «The Secret Online Weapons Store That'll Sell Anyone Anything». En: *Gizmodo*, 19 de julio de 2012; Adrian Chen. «Now You Can Buy Guns on the Online Underground Marketplace». En: *Gawker*, 27 de enero de 2012. <<

[30] Sam Biddle. «The Secret Online Weapons Store That'll Sell Anyone Anything». En: *Gizmodo*, 19 de julio de 2012. <<

[31] Greenberg. «Meet the “Assassination Market” Creator Who’s Crowdfunding Murder with Bitcoins». <<

[32] Dylan Love. «How to Hire an Assassin on the Secret Internet for Criminals». En: *Business Insider*, 16 de marzo de 2013. <<

[33] Joel Falconer. «*Mail*-Order Drugs, Hitmen, and Child Porn: A Journey into the Dark Corners of the Deep Web». En: *Next Web*, 8 de octubre de 2012. <<

[34] Patrick Howell O’Neill. «Feds Dismantle Massive Deep Web Child Porn *Ring*». En: *Daily Dot*, 19 de marzo de 2014. <<

[35] *Thorn Blog*, http://www.wearethorn.org/child-*trafficking*-statistics/. <<

[36] Testimonio de Ernie Allen, presidente del Centro Nacional de Niños Desaparecidos y Víctimas de Abusos ante el Comité sobre la Explotación Sexual Comercial y el Tráfico Sexual de Menores en Estados Unidos del Institute of Medicine, National Academies, disponile en http://storage.cloversites.com/thedaughterproject/documents/NCMEC%20report%20to%20congress%2001-04-12.pdf; http://www.nap.edu/catalog.php?record_id=18358 <<

[37] Personal de NPR. «Courts Take a Kinder *Look* at Victims of Child Sex Trafficking». NPR.org, 1 de marzo de 2014. <<

[38] Thorn Staff. «Child Sex Trafficking and Exploitation Online: Escort Websites», 11 de marzo de 2014; National Human Trafficking Resource Center. «Residential Brothels». <<

[39] Mark Latonero. «The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking». Universidad de California del Sur. <<

[40] Shared Hope International. «Demanding Justice Project Benchmark Assessment 2013», pág. 13; Michelle Goldberg. «Sex Slave Outrage». En: *Daily Beast*, 9 de diciembre de 2010. <<

[41] Puede consultarse un magnífico reportaje acerca del mercado negro internacional de órganos humanos en la serie de cuatro partes que *Der Spiegel* publicó sobre el tema, disponible en inglés en http://www.spiegel.de/international/world/the-illegal-trade-in-organ-is-fueled-by-desperation-and-*growing*-a-847473.html. <<

[42] Casey Chan. «Here's How Much *Body* Parts Cost on the Black Market». En: *Gizmodo*, 23 de abril de 2012. <<

[43] National Kidney Foundation. «Organ Donation and Transplantation Statistics», 8 de septiembre de 2014. <<

[44] Jeneen Interlandi. «Organ Trafficking Is No Myth». En: *Newsweek*, 9 de enero de 2009. <<

[45] Damien Gayle. «An Organ Is Sold Every Hour, WHO Warns: Brutal Black Market on the Rise Again Thanks to Diseases of Affluence». En: *Mail Online*, 27 de mayo de 2012. <<

[46] Ulrike Putz. «Organ Trade Thrives Among Desperate Syrian Refugees in Lebanon». En: *Spiegel Online*, 11 de diciembre de 2013; Jiayang Fan. «Can China *Stop* Organ Trafficking?». En: *New Yorker*, 10 de enero de 2014. <<

[47] Esther Inglis-Arkell. «How Do You Buy Organs on the Black Market?». En: *io9*, 26 de marzo de 2012. <<

[48] Dan Bilefsky. «Black Market for *Body* Parts Spreads in Europe». En: *New York Times*, 28 de junio de 2012. <<

[49] Denis Campbell y Nicola Davison. «Illegal Kidney Trade *Booms* as New Organ Is "Sold Every Hour"». En: *Guardian*, 27 de mayo de 2012. <<

[50] «9 on Trial in China over Teenager’s Sale of Kidney for iPad and iPhone». CNN, 10 de agosto de 2012. <<

[51] Centro Europeo de Ciberdelincuencia. «Explotación sexual infantil en línea», octubre de 2013. <<

[52] Paul Gallagher. «Live Streamed Videos of Abuse and Pay-per-View Child Rape Among “Disturbing” Cybercrime Trends, Europol Report Reveals». En: *Independent*, 16 de octubre de 2013; Paul Peachey. «Number of UK Paedophiles “Live-Streaming” Child Abuse Films Soars, Warns CEOP». En: *Independent*, 1 de julio de 2013. <<

[53] Ann Cahill. «New Age of Cybercrime: Live Child Rapes, Sextortion, and Advanced Malware». En: *Irish Examiner*, 11 de febrero de 2014. <<

[54] «How Does Bitcoin Work?». En: *Economist*, 11 de abril de 2013. <<

[55] Nick Farrell. «Understanding Bitcoin and Crypto Currency». En: *Tech Radar*, 7 de abril de 2014. <<

[56] Joshua Brustein. «Bitcoin May Not Be So Anonymous, After All». En: *Bloomberg Businessweek*, 27 de agosto 2013. <<

[57] Alan Yu. «How Virtual Currency Could Make It Easier to Move Money». NPR.org, 15 de enero de 2014. <<

[58] Robin Sidel, Eleanor Warnock y Takashi Mochizuki. «Almost Half a Billion Worth of Bitcoins Vanish». En: *Wall Street Journal*, 1 de marzo de 2014. <<

[59] Marc Santora, William K. Rashbaum y Nicole Perlroth. «Liberty Reserve Operators Accused of Money Laundering». En: *New York Times*, 28 de mayo de 2013. <<

[60] Oficina del Fiscal General de Southern New York de Estados Unidos. «Liberty Reserve Information Technology Manager Pleads Guilty in Manhattan Federal Court». Nota de prensa del Departamento de Justicia de Estados Unidos, 23 de septiembre de 2014. <<

[61] Andy Greenberg. «Darkcoin, the Shadowy Cousin of Bitcoin, Is Booming». En: *Wired*, 21 de mayo de 2014. <<

[62] Andy Greenberg. «“Dark Wallet” Is About to Make Bitcoin Money Laundering Easier Than Ever». En: *Wired*, 29 de abril de 2014. <<

[63] James Vincent. «Irish Man Arrested as “the Largest Facilitator of Child Porn on the Planet”». En: *Independent*, 5 de agosto de 2013. <<

[64] Kevin Poulsen. «FBI Admits It Controlled Tor Servers Behind Mass Malware Attack». En: *Wired*, 13 de septiembre de 2013. <<

[65] Solutionary, una empresa de seguridad de NTT. *Security Engineering Research Team (SERT) Quarterly Threat Intelligence Report*, 2013, pág 8, http://www.solutionary.com. <<

[66] *Ibíd.* <<

[67] «Cybercriminals Today Mirror Legitimate Business Processes», pág. 4. <<

[68] Simson Garfinkel. «The Criminal Cloud». En: *MIT Technology Review*, 17 de octubre de 2011. <<

[69] Misha Glenny. *DarkMarket: Cyberthieves, Cybercops, and You*. Nueva York: Knopf, 2011, pág. 203 <<

[70] Danny Yadron. «Symantec Fingers Most Advanced Chinese *Hacker* Group». En: *Digits* (blog), *Wall Street Journal*, 17 de septiembre de 2013. <<

[71] Kim Zetter. «State-Sponsored *Hacker* Gang Has a Side Gig in Fraud». En: *Wired*, 17 de septiembre de 2013. <<

[72] Kim Zetter. «Cops Pull Plug on Rent-a-Fraudster Service for Bank Thieves». En: *Wired*, 19 de abril de 2010. <<

[73] Ablon, Libicki y Golay. «Markets for Cybercrime Tools and Stolen Data», pág. 4. <<

[74] Forward-Looking Threat Research Team. «Deepweb and Cybercrime», pág. 9; Ablon, Libicki y Golay. «Markets for Cybercrime Tools and Stolen Data», pág. 4 <<

[75] Taylor Armerding. «Dark Web: An Ever-More-Comfortable Haven for Cyber Criminals». En: *CSO Online*, 28 de marzo de 2014. <<

[76] Donna Leinwand Leger y Anna Arutunyan. «How the Feds Brought Down a Notorious Russian *Hacker*». En: *USA Today*, 5 de marzo de 2014. <<

[77] Dan Raywood. «New Version of Bugat Trojan Was Payload in LinkedIn *Spam* and Not Zeus». En: *SC Magazine UK*, 12 de octubre de 2010. <<

[78] Robert McMillan. «New Russian Botnet Tries to Kill Rival». En: *Computerworld*, 9 de febrero de 2010. <<

[79] Kurt Eichenwald. «The $500,000,000 Cyber-Heist». En: *Newsweek*, 13 de marzo de 2014. <<

[80] Gregory J. Millman. «Cybercriminals Work in a Sophisticated Market Structure». En: *Wall Street Journal*, 27 de junio de 2013. <<

[81] Dana Liebelson. «All About Blackshades, the Malware That Lets *Hackers* Watch You Through Your Webcam». En: *Mother Jones*, 21 de mayo de 2014. <<

[82] «Syrian Activists Targeted with BlackShades Spy *Software*». En: *The Citizen Lab*, 19 de junio de 2012. <<

[83] Gregg Keizer. «Google to Pay Bounties for Chrome Browser Bugs». En: *Computerworld*, 29 de enero de 2010. <<

[84] Brian Krebs. «Meet Paunch: The Accused Author of the BlackHole Exploit Kit». En: *Krebs on Security*, 6 de diciembre de 2013. <<

[85] Nicole Perlroth y David E. Sanger. «Nations Buying as *Hackers* Sell Flaws in Computer Code». En: *New York Times*, 13 de julio de 2013. <<

[86] Andy Greenberg. «Shopping for Zero-Days: A Price List For *Hackers*' Secret *Software* Exploits». En: *Forbes*, 23 de marzo de 2012. <<

[87] Brian Krebs. «How Many Zero-Days Hit You Today». En: *Krebs on Security*, 13 de diciembre de 2013. <<

[88] Josh Sanburn. «How Exactly Do Cyber Criminals Steal $78 Million?». En: *Time*, 3 de julio de 2012. <<

[89] Simonite. «Stuxnet Tricks Copied by Computer Criminals». <<

[90] «The Child Porn PC Virus». En: *Week*, 10 de noviembre de 2009. <<

[91] FBI. «GameOver Zeus Botnet Disrupted», 2 de junio de 2014. <<

[92] «Grappling with the ZeroAccess Botnet», 30 de septiembre de 2013. <<

[93] Ian Steadman. «The Russian Underground Economy Has Democratised Cybercrime». En: *Wired UK*, 2 de noviembre de 2012. <<

[94] «Computer Says No». En: *Economist*, 22 de junio de 2013; Perlroth y Hardy. «Bank Hacking Was the Work of Iranians». <<

[95] Chris Brook. «Meetup.com Back Online After DDoS Attacks, Extortion Attempt». En: *Threat Post*, 5 de marzo de 2014; Pierluigi Paganini. «Botnet Authors Use Evernote Account as C&C Server». En: *Security Affairs*, 31 de marzo de 2013. <<

[96] Mathew J. Schwartz. «Malware Toolkits Generate Majority of Online Attacks». En: *Dark Reading*, 18 de enero de 2011. <<

[97] David Wismer. «Hand-to-Hand Combat with the Insidious “FBI MoneyPak Ransomware Virus”». En: *Forbes*, 6 de febrero de 2013. <<

[98] EnigmaSoftware. «Abu Dhabi Police GHQ Ransomware». <<

[99] Mark Ward. «Crooks “Seek Ransomware Making Kit”». BBC News, 10 de diciembre de 2013. <<

[100] Dave Jeffers. «Crime Pays Very Well: CryptoLocker Grosses up to $30 Million in Ransom». En: *PCWorld*, 20 de diciembre de 2013. <<

[101] Dennis Fisher. «Device-Locking Ransomware Moves to Android». En: *ThreatPost*, 7 de mayo de 2014. <<

[102] Violet Blue. «CryptoLocker’s Crimewave: A Trail of Millions in Laundered Bitcoin». En: *ZDNet*, 22 de diciembre de 2013; Bree Sison. «Swansea Police Pay Ransom After Computer System Was Hacked». CBS Boston, 18 de noviembre de 2013. <<

[1] Joanne Kimberlin. «High-Tech “Repo Man” Keeps Car Payments Coming». En: *USA Today*, 29 de noviembre de 2005; Christina Rosales. «Police: Fired Worker Disabled Cars via Web». En: *Statesman*, 17 de marzo de 2010; Kevin Poulsen. «*Hacker* Disables More Than 100 Cars Remotely». En: *Wired*, 17 de marzo de 2010. <<

[2] Michael Singer. «PC Milestone-Notebooks Outsell Desktops». En: *CNET*, 3 de junio de 2005; Salvador Rodriguez. «More Tablets to Be Sold Than PCs in 2015, Report Says». ChicagoTribune.com, 8 de julio de 2014. <<

[3] «2014: Mobiles “to Outnumber People”». BBC News, 9 de mayo de 2013. <<

[4] Pew Research Center. «Digital Life in 2025», marzo de 2014; Pew Research Center’s Internet & American Life Project. «Internet of Things», acceso realizado el 21 de julio de 2014, http://www.pewinternet.org/. <<

[5] Lopez Research. «An Introduction to the Internet of Things». Cisco, noviembre de 2013. <<

[6] Terril Yue Jones. «A Law of Continuing Returns». En: *Los Angeles Times*, 17 de abril de 2005. <<

[7] Olga Kharif. «Trillions of Smart Sensors Will Change Life». En: *Bloomberg*, 4 de agosto de 2013. <<

[8] Neil Gershenfeld y J. P. Vasseur. «As Objects Go Online». En: *Foreign Affairs*, marzo/abril de 2014. <<

[9] Laurie J. Flynn. «As World Runs Out of I. P. Addresses, Switch to IPv6 Nears». En: *New York Times*, 14 de febrero de 2011. <<

[10] Andrew G. Blank. *TCP/IP Foundations*. Hoboken, Nueva Jersey: John Wiley & Sons, 2006, pág. 233. <<

[11] John Martellaro. «A Layman's Guide to the IPv6 Transition». En: *The Mac Observer*, 31 de enero de 2012; Robert Krulwich. «Which Is Greater, the Number of Sand Grains on Earth or Stars in the Sky?». NPR, 17 de septiembre de 2012. <<

[12] Steve Leibson. «IPV6: How Many IP Addresses Can Dance on the Head of a Pin». En: *EDN Network*, 28 de marzo de 2008; «The Internet of Things», Cisco Infographic. <<

[13] «IPv6-What Is It, Why Is It Important, and Who Is in Charge?» (documento preparado para la junta ejecutiva de ICANN y todos los registros regionales de Internet), octubre de 2009. <<

[14] Dave Evans. «The Internet of Things». Cisco, abril de 2011. <<

[15] McKinsey Global Institute. *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy*. Mayo de 2013, pág. 55, MGI_Disruptive_technologies_*Full*_report_May2013.pdf. <<

[16] *Emerging Cyber Threats* (presentado por el Georgia Institute of Technology y el Georgia Tech Research Institute en la Cumbre de Ciberseguridad y Tecnología de Georgia de 2013), pág. 4. <<

[17] Global Strategy and Business Development, Freescale and Emerging Technologies, ARM. *What the Internet of Things (IoT) Needs to Become a Reality.* Mayo de 2014. <<

[18] Marcus Wohlsen. «Forget Robots. We’ll Soon Be Fusing Technology with Living Matter». En: *Wired*, 27 de mayo de 2014. <<

[19] Robert Muir. «Thirsty Plants Can Twitter for *Water* with New Device». Reuters, 26 de marzo de 2009; https://twitter.com/pothos; Rachel Metz. «In San Francisco, a House with Its Own Twitter Feed». En: *MIT Technology Review*, 21 de mayo de 2013. <<

[20] Gershenfeld y Vasseur. «As Objects Go Online». <<

[21] Alan Yu. «More Than 300 Sharks in Australia Are Now on Twitter». NPR. org, 1 de enero de 2014. <<

[22] Alexis C. Madrigal. «Welcome to the Internet of Thingies: 61.5% of Web Traffic Is Not Human». En: *Atlantic*, 12 de diciembre de 2013. <<

[23] M. Presser y S. Krco. *Initial Report on IoT Applications of Strategic Interest*, Internet of Things Initiative, 8 de octubre de 2011, pág. 48. <<

[24] Annalee Newitz. «The RFID Hacking Underground». En: *Wired*, mayo de 2006. <<

[25] Francis Brown y Bishop Fox. «RFID Hacking» (documento presentado en Black Hat USA, Las Vegas, Nevada, 1 de agosto de 2013). <<

[26] «*Hackers* Could Clone Your Office Key Card… from Your Pocket». NBC News, 25 de julio de 2013. <<

[27] Andy Greenberg. «*Hacker*'s Demo *Shows* How Easily Credit Cards Can Be Read Through Clothes and Wallets». En: *Forbes*, 30 de enero de 2012. <<

[28] Nate Anderson. «RFID Chips Can Carry Viruses». En: *Ars Technica*, 15 de marzo de 2006. <<

[29] Juniper Research. «1 in 5 *Smartphones* will have NFC by 2014, Spurred by Recent Breakthroughs: New Juniper Research Report», 14 de abril de 2011. <<

[30] Andy Greenberg. «*Hacker* Demos Android App That Can Wirelessly Steal and Use Credit Cards' Data». En: *Forbes*, 27 de julio de 2012. <<

[31] Lance Whitney. «Latest Google Wallet *Hack* Picks Your Pocket». En: *CNET*, 10 de febrero de 2012; Evan Applegate. «Have Fingers, 30 Seconds? You, Too, Can *Hack* Google Wallet». En: *Bloomberg Businessweek*, 13 de febrero de 2012. <<

[32] Gabrielle Taylor. «Have an NFC-Enable Phone? This *Hack* Could Hijack It». En: *WonderHowTo*, acceso realizado el 1 de julio de 2014. <<

[33] Lisa Vaas. «Android NFC *Hack* Lets Subway Riders Evade Fares». En: *Naked Security*, 24 de septiembre de 2012. <<

[34] Kate Murphy. «Protecting a Cellphone Against *Hackers*». En: *New York Times*, 25 de enero de 2012; Tu C. Neim. «Bluetooth and Its Inherent Security Issues». SANS Institute InfoSec Reading Room, 4 de noviembre de 2002. <<

[35] Catherine Crump y Matthew Harwood. «Invasion of the Data Snatchers: Big Data and the Internet of Things Means the Surveillance of Everything». En: *Blog of Rights*, 25 de marzo de 2014. <<

[36] «Snapshot Common Questions». Sitio web de Progressive: http://www.progressive.com/auto/snapshot-common-questions/. <<

[37] Rolfe Winkler. «Google Predicts Ads in Odd *Spots* Like Thermostats». En: *Digits* (blog), *Wall Street Journal*, 21 de mayo de 2014. <<

[38] Brian Brady. «Prisoners “to Be Chipped like Dogs”». En: *Independent*, 13 de enero de 2008. <<

[39] David Rosen. «Big Brother Invades Our Classrooms». En: *Salon,* 8 de octubre de 2012. <<

[40] David Kravets. «Student Suspended for Refusing to Wear a School-Issued RFID Tracker». En: *Wired*, 21 de noviembre de 2012. <<

[41] Aaron Katersky y Josh Haskell. «NY Mom Accused of Growing $3M Marijuana Business». En: *Good Morning America*, 6 de junio de 2013; Glenn Smith. «Marijuana Bust Shines *Light* on Utilities». En: *Post and Courier*, 29 de enero de 2012. <<

[42] Spencer Ackerman. «CIA Chief: We’ll Spy on You Through Your Dishwasher». En: *Wired*, 15 de marzo de 2012. <<

[43] Neil J. Rubenking. «Black Hat: Don’t Plug Your Phone into a Charger You Don’t Own». *PCMag*, 1 de agosto de 2013. <<

[44] «Public Charging Stations Help *Smartphone* Users, but Also Open a New Avenue for Hacking». En: *Daily News* (edición de Nueva York), 13 de agosto de 2013. <<

[45] Simon Sharwood. «DON’T BREW THAT CUPPA! Your Kettle Could Be a SPAMBOT». En: *Register*, 29 de octubre de 2013; Adam Clark Estes. «Russian Authorities Seize Goods from China Implanted with Spy Chips». En: *Gizmodo*, 29 de octubre de 2013. <<

[46] Erik Sherman. «Hacked from China: Is Your Kettle Spying on You?». CBS News, 1 de noviembre de 2013. <<

[47] Klint Finley. «Why Tech’s Best Minds Are Very Worried About the Internet of Things». En: *Wired*, 19 de mayo de 2014. <<

[1] David Kravets. «School District Allegedly Snapped Thousands of Student Webcam Spy Pics». En: *Wired*, 16 de abril de 2010; Kashmir Hill. «Lower Merion School District and Blake Robbins Reach a Settlement in Spycamgate». En: *Forbes*, 11 de octubre de 2010; John P. Martin. «L. Merion Smearing Former IT Chief, Lawyer Says». Philly.com, 5 de mayo de 2010. <<

[2] Suzan Clarke. «Pa. School Faces FBI Probe». ABC News, 22 de febrero de 2010. <<

[3] Loretta Chao. «Cisco Poised to Help China Keep an Eye on Its Citizens». En: *Wall Street Journal*, 5 de julio de 2011. <<

[4] John Biggs. «DARPA Builds a 1.8-Gigapixel Camera». En: *TechCrunch*, 28 de enero de 2013. <<

[5] «Fighting Terrorism in New York City». En: *60 Minutes*, 26 de septiembre de 2011. <<

[6] «Miss Teen USA: Screamed upon Learning She Was “Sextortion” Victim». CNN, 28 de septiembre de 2013. <<

[7] Aaron Katersky. «Miss Teen USA 1 of “Half-Million Blackshades” *Hack* Victims». ABC News, 19 de mayo de 2014. <<

[8] Amy Wagner. «*Hacker* Hijacks *Baby* Monitor». Fox News, 22 de abril de 2014. <<

[9] «Parents Left Terrified After Man Hacked Their *Baby* Monitor and Yelled Abuse at Them and Their 2-Year-Old Daughter». En: *Mail Online*, 13 de agosto de 2013. <<

[10] Kim Zetter. «Popular Surveillance Cameras Open to *Hackers*, Researcher Says». En: *Wired*, 15 de mayo de 2012. <<

[11] Kelly Jackson Higgins. «Millions of Networked Devices in Harm's Way». En: *Dark Reading*, 29 de enero de 2013. <<

[12] Katie Notopoulos. «Somebody's Watching: How a Simple Exploit Lets Strangers Tap into Private Security Cameras». En: *Verge*, 3 de febrero de 2012. <<

[13] Jim Finkle. «US Security Expert Says Surveillance Cameras Can Be Hacked». Reuters, 18 de junio de 2013. <<

[14] Mark Buttler. «Crown Casino Hi-Tech Scam Nets $32 Million». *Herald Sun* (Melbourne), March 14, 2013. <<

[15] Kim Zetter. «Crooks Spy on Casino Card Games with Hacked Security Cameras, Win $33M». En: *Wired*, 15 de marzo de 2013. <<

[16] Robert N. Charette. «This Car Runs on Code». En: *IEEE Spectrum*, 1 de febrero de 2009. <<

[17] Ibíd., Chris Bryant. «Manufacturers Respond to Car-Hacking Risk». En: *Financial Times*, 22 de marzo de 2013. <<

[18] Craig Timberg. «Web-Connected Cars Bring Privacy Concerns». En: *Washington Post*, 5 de marzo de 2013. <<

[19] «GPS Users Beware, Big Auto Is Watching: Report». CNBC.com, 9 de enero de 2014. <<

[20] John R. Quain. «Changes to OnStar’s Privacy Terms Rile Some Users». En: *Wheels* (blog), *New York Times*, 22 de septiembre de 2011. <<

[21] Declan McCullagh y Anne Broache. «FBI Taps Cell Phone Mic as Eavesdropping Tool». En: *CNET*, 1 de diciembre de 2006; Bruno Waterfield y Matthew Day. «EU Has Secret Plan for Police to "Remote *Stop*" Cars». En: *Telegraph*, 29 de enero de 2014. <<

[22] Jeff Bennett. «GM Adds 8.45 Million Vehicles to North America Recall». En: *Wall Street Journal*, 30 de junio de 2014; Christopher Jensen. «An Increase in Recalls Goes Beyond Just G. M.». En: *New York Times*, 29 de mayo de 2014. <<

[23] James R. Healey. «Toyota Deaths Reported to Safety Database Rise to 37». En: *USA Today*, 17 de febrero de 2010. <<

[24] Phil Baker. «*Software* Bugs Found to Be Cause of Toyota Acceleration Death». En: *Daily Transcript*, 4 de noviembre de 2013; Junko Yoshida. «Acceleration Case: Jury Finds Toyota Liable». En: *EETimes*, 24 de octubre de 2013. <<

[25] Jerry Hirsch. «Toyota Admits Misleading Regulators, Pays $1.2-Billion Federal Fine». En: *Los Angeles Times*, 19 de marzo de 2014. <<

[26] Victoria Woollaston. «Forget Carjacking, the Next Big Threat Is Car-HACKING». En: *Mail Online*, 8 de mayo de 2014. <<

[27] William Pentland. «Car-Hacking Goes Viral in London». En: *Forbes*, 20 de mayo de 2014; Thomas Cheshire. «Thousands of Cars Stolen Using Hi-Tech Gadgets». En: *Sky News*, 8 de mayo de 2014. <<

[28] Sebastian Anthony. «*Hackers* Can Unlock Cars via SMS». *ExtremeTech*, 28 de julio de 2011; Robert McMillan. «"War Texting" Lets *Hackers* Unlock Car Doors Via SMS». En: *CSO Online*, 27 de julio de 2011. <<

[29] Rebecca Boyle. «Trojan-Horse MP3s Could Let *Hackers* Break into Your Car Remotely, Researchers Find». En: *Popular Science*, 14 de marzo de 2011. <<

[30] Victoria Woollaston. «The $20 Handheld Device That *Hacks* a CAR-and Can Control the Brakes». En: *Mail Online*, 6 de febrero de 2014. <<

[31] John Markoff. «Researchers *Hack* into Cars' Electronics». En: *New York Times*, 9 de marzo de 2011; Chris Philpot. «Can Your Car Be Hacked?». En: *Car and Driver*, agosto de 2011; Andy Greenberg. «*Hackers* Reveal Nasty New Car Attacks-with Me Behind the Wheel». En: *Forbes*, 24 de julio de 2013; Dan Goodin. «Tampering with a Car's Brakes and Speed by Hacking Its Computers: A New How-To». En: *Ars Technica*, 29 de julio de 2013. <<

[32] Paul A. Eisenstein. «Spying, Glitches Spark Concern for Driverless Cars». CNBC.com, 8 de febrero de 2014 <<

[33] Sebastian Anthony. «Google's Self-Driving Car Passes 700,000 Accident-Free Miles, Can Now Avoid Cyclists, *Stop* at Railroad Crossings». En: *ExtremeTech*, 29 de abril de 2014; John Markoff. «Google's Next Phase in Driverless Cars: No Steering Wheel or Brake Pedals». En: *New York Times*, 27 de mayo de 2014. <<

[34] Lance Whitney. «FBI: Driverless Cars Could Become “Lethal Weapons”». En: *CNET*, 16 de julio de 2014. <<

[35] Ms. Smith. «Most “Hackable” Vehicles Are Jeep, Escalade, Infiniti, and Prius». En: *Network World*, 3 de agosto de 2014. <<

[36] Ina Fried. «Tesla Hires *Hacker* Kristin Paget to, Well, Secure Some Things». En: *Re/code*, 7 de febrero de 2014. <<

[37] Transparency Market Research. «Home Automation Market (Lighting, Safety and Security, Entertainment, HVAC, Energy Management)-Global Industry Analysis, Size, Share, Growth, Tends, and Forecast, 2013−2019», 30 de septiembre de 2013. <<

[38] Kashmir Hill. «When “Smart Homes” Get Hacked: I Haunted a Complete Stranger’s House via the Internet». En: *Forbes*, 26 de julio de 2013. <<

[39] Daniel Miessler. «HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack». HP, 29 de julio de 2014. <<

[40] Arrayent. «Internet of Things Toys with Mattel», http://www.arrayent.com/internet-of-*things*-case-studies/*connecting*-toys-with-mattet/Disney Research. «CALIPSO: Internet of Things», http://www.disneyresearch.com/project/calipso-internet-of-*things*/. <<

[41] Heather Kelly. «“Smart Homes” Are Vulnerable, Say *Hackers*». CNN, 2 de agosto de 2013 <<

[42] Dan Goodin. «Welcome to the “Internet of Things”, Where Even *Lights* Aren’t *Hacker* Safe». En: *Ars Technica*, 13 de agosto de 2013. <<

[43] Jane Wakefield. «Experts *Hack* Smart LED *Light* Bulbs». BBC News, 8 de julio de 2014; Leo King. «Smart Home? These Connected LED *Light* Bulbs Could Leak Your Wi-Fi Password». En *Forbes*, 9 de julio de 2014. <<

[44] Andy Greenberg. «An Eavesdropping Lamp That Livetweets Private Conversations». En: *Wired*, 23 de abril de 2014. <<

[45] Hill. «When “Smart Homes” Get Hacked». <<

[46] Paul Roberts. «Breaking and Entering». En: *The Security Ledger*, 25 de julio de 2013. <<

[47] Ms. Smith. «500,000 Belkin WeMo Users Could Be Hacked; CERT Issues Advisory». En: *Network World*, 18 de febrero de 2014. <<

[48] Kashmir Hill. «How Your Security System Could Be Hacked to Spy on You». En: *Forbes*, 23 de julio de 2014. <<

[49] Ms. Smith. «Hacking and Attacking Automated Homes». En: *Network World*, 25 de junio de 2013. <<

[50] Nancy Trejos. «Hilton Lets Guests Pick Rooms, Use *Smartphones* as Keys». En: *USA Today*, 29 de julio de 2014. <<

[51] Michael Wolf. «3 Reasons 87 Million Smart TVs Will Be Sold in 2013». En: *Forbes*, 25 de febrero de 2013. <<

[52] Lorenzo Franceschi-Bicchierai. «Your Smart TV Could Be Hacked to Spy on You». En: *Mashable*, 2 de agosto de 2013; Dan Goodin. «How an Internet-Connected Samsung TV Can Spill Your Deepest Secrets». En: *Ars Technica*, 12 de diciembre de 2012. <<

[53] Ellie Zolfagharifard. «Criminals Use a Fridge to Send Malicious *Emails* in First Ever Home *Hack*». En: *Mail Online*, 17 de enero de 2014. <<

[54] «*Spam* in the Fridge». En: *Economist*, 25 de enero de 2014. <<

[55] Dan Goodin. «“Internet of Things” Is the New Windows XP-Malware’s Favorite Target». En: *Ars Technica*, 2 de abril de 2014. <<

[56] *Utility-Scale Smart Meter Deployments*, informe de IEE report, agosto de 2013, pág. 3; Chris Choi. «Smart Meters Are Heading to Every Home in Britain». ITV News, 8 de julio de 2014. <<

[57] Jordan Robertson. «Your Outlet Knows: How Smart Meters Can Reveal Behavior at Home, What We Watch on TV». En: *Bloomberg*, 10 de junio de 2014. <<

[58] Brian Krebs. «FBI: Smart Meter *Hacks* Likely to Spread». En: *Krebs on Security*, 9 de abril de 2012 <<

[59] Katie Fehrenbacher. «Smart Meter Worm Could Spread like a Virus». En: *Gigaom*, 31 de julio de 2009. <<

[60] Rolfe Winkler. «What Google Gains from Nest Labs». En: *Wall Street Journal*, 15 de enero de 2014. <<

[61] Marcus Wohlsen. «What Google Really Gets out of Buying Nest for $3. 2 Billion». En: *Wired*, 14 de enero de 2014. <<

[62] Richard Lawler. «Nest Learning Thermostat Has Its Security Cracked Open by GTVHacker». En *Engadget*, 23 de junio de 2014. <<

[63] Edward C. Baig. «Nest Halts Sales, Issues Warning on Smoke Detector». En: *USA Today*, 3 de abril de 2014. <<

[64] Hill. «How Your Security System Could Be Hacked to Spy on You». <<

[65] Armen Keteyian. «Digital Photocopiers Loaded with Secrets». CBS News, 19 de abril de 2010. <<

[66] Dan Ilett. «*Hackers* Use Google to Access Photocopiers». En: *ZDNet*, 24 de septiembre de 2004. <<

[67] Graham Cluley. «HP Printer Security Flaw Allows *Hackers* to Extract Passwords». GrahamCluley.com, 7 de agosto de 2013. <<

[68] «Exclusive: Millions of Printers Open to Devastating *Hack* Attack, Researchers Say». NBC News, 29 de noviembre de 2011; Sebastian Anthony. «Tens of Millions of HP LaserJet Printers Vulnerable to Remote Hacking». En: *ExtremeTech*, 29 de noviembre de 2011. <<

[69] Nicole Perlroth. «Flaws in Videoconferencing Systems Make Boardrooms Vulnerable». En: *New York Times*, 22 de enero de 2012. <<

[70] Brock Parker. «*Hackers* Convert MIT Building in Giant Tetris Video Game». Boston.com, 24 de abril de 2012. <<

[71] Brian Krebs. «Fazio Mechanical Services». En: *Krebs on Security*, 12 de febrero de 2014; Gregory Wallace. «HVAC Vendor Eyed as Entry Point for Target Breach». En: *CNNMoney*, 7 de febrero de 2014; Danny Yadron y Paul Ziobro. «Before Target, They Hacked the Heating Guy». En: *Digits* (blog), *Wall Street Journal*, 5 de febrero 2014. <<

[72] Dan Goodin. «Epic Target *Hack* Reportedly Began with Malware-Based Phishing *E-Mail*». En: *Ars Technica*, 12 de febrero de 2014; Comité de Comercio, Ciencia y Transporte del Senado de Estados Unidos. *A «Kill Chain» Analysis of the 2013 Target Data Breach*, Majority Staff Report for Chairman Rockefeller, 26 de marzo de 2014. <<

[73] Kim Zetter. «The Malware That Duped Target Has Been Found». En: *Wired*, 16 de enero de 2014. <<

[74] Sean Gallagher. «Vulnerabilities Give *Hackers* Ability to Open Prison Cells from Afar». En: *Ars Technica*, 7 de noviembre de 2011; Shaun Waterman. «Prisons Bureau Alerted to Hacking into Lockups». En: *Washington Times*, 6 de noviembre de 2011. <<

[75] Kim Zetter. «Prison Computer “Glitch” Blamed for Opening Cell Doors in Maximum-Security Wing». En: *Wired*, 16 de agosto de 2013. <<

[76] Siobhan Gorman. «China *Hackers* Hit U. S. Chamber». En: *Wall Street Journal*, 21 de diciembre de 2011. <<

[77] Goodman. «Power of Moore’s Law in a World of Geotechnology». <<

[78] Marshall McLuhan. *Comprender los medios de comunicación: las extensiones del ser humano* (traducción de Patrick Ducher). Barcelona: Paidós, 2009. <<

[79] Elizabeth Dwoskin. «They’re Tracking When You Turn *Off* the *Lights*». En: *Wall Street Journal*, 20 de octubre de 2014. <<

[80] «Outdoor Lighting». Echelon, https://www.echelon.com/applications/street-*lighting*/. <<

[81] Mark Prigg. «New York’s Traffic *Lights* HACKED». En: *Mail Online*, 30 de abril de 2014. <<

[82] Erica Naone. «Hacking the Smart Grid». En: *MIT Technology Review*, 2 de agosto de 2010. <<

[83] Reuters. «“Smart” Technology Could Make Utilities More Vulnerable to *Hackers*». En: *Raw Story*, 16 de julio de 2014. <<

[1] Amber Case. «We Are All *Cyborgs* Now». Conferencia TED Talk, diciembre de 2010. <<

[2] «Text Message/Mobile *Marketing*». WebWorld2000, http://www.webworld2000.com/. <<

[3] Marcelo Ballve. «Wearable Gadgets Are Still Not Getting the Attention They Deserve-Here's Why They Will Create a Massive New Market». En: *Business Insider*, 29 de agosto de 2013. <<

[4] «How Safe Is Your Quantified Self? Tracking, Monitoring, and Wearable Tech». En: *Symantec Security Response*, 30 de julio de 2014. <<

[5] «Google Partners with Ray-Ban, Oakley for New Glass Designs». NBC News, 24 de marzo de 2014; Deloitte, *Technology*, *Media*, *and Telecommunications Predictions*, *2014*, pág. 10. <<

[6] Richard Gray. «The Places Where Google Glass Is Banned». En: *Telegraph*, 4 de diciembre de 2013. <<

[7] Andy Greenberg. «Google Glass Has Already Been Hacked by Jailbreakers». En: *Forbes*, 26 de abril de 2013. <<

[8] Mark Prigg. «Google Glass HACKED to Transmit Everything You See and Hear: Experts Warn “the Only Thing It Doesn’t Know Are Your Thoughts”». En: *Mail Online*, 2 de mayo de 2013. <<

[9] John Zorabedian. «Spyware App Turns the Privacy Tables on Google Glass Wearers». En: *Naked Security*, 25 de marzo de 2014. <<

[10] Katherine Bourzac. «Contact Lens Computer: Like Google Glass, Without the Glasses». En: *MIT Technology Review*, 7 de junio de 2013. <<

[11] Leo King. «Google Smart Contact Lens Focuses on Healthcare Billions». En: *Forbes*, 15 de julio de 2014. <<

[12] Bourzac. «Contact Lens Computer». <<

[13] N. M. van Hemel y E. E. van der Wall. «8 October 1958, D Day for the Implantable Pacemaker». En: *Netherlands Heart Journal* 16, n.º S1 (octubre de 2008): S3-S4. <<

[14] Ben Gruber. «First Wi-Fi Pacemaker in US Gives Patient Freedom». Reuters, 10 de agosto de 2009. <<

[15] Michael Rushanan *et al*. «SoK: Security and Privacy in Implantable Medical Devices and *Body* Area Networks». En: *SP '14 Proceedings of the 2014 IEEE Symposium on Security and Privacy* (2014), págs. 524-539; Yeun-Ho Joung. «Development of Implantable Medical Devices: From an Engineering Perspective». En: *International Neurourology Journal* 17, n.º 3 (septiembre de 2013), págs. 98-106; «IMD Shield: Securing Implantable Medical Devices», http://groups.csail.mit.edu/. <<

[16] Thomas M. Burton. «Medical Device Recalls Nearly Doubled in a Decade». En: *Wall Street Journal*, 21 de marzo de 2014. <<

[17] H. Alemzadeh *et al*. «Analysis of Safety-Critical Computer Failures in Medical Devices». En: *IEEE Security Privacy* 11, n.º 4 (julio de 2013), págs. 14-26, doi:10.1109/ MSP.2013.49. <<

[18] Kim Zetter. «It’s Insanely Easy to *Hack* Hospital Equipment». En: *Wired*, 25 de abril de 2014; David Talbot. «Computer Viruses Are “Rampant” on Medical Devices in Hospitals». En: *MIT Technology Review*, 17 de octubre de 2012. <<

[19] «Medical Devices Hard-Coded Passwords». ICS-CERT, http://ics-cert.uscert.gov/alerts/ICS-ALERT-13-164-01. <<

[20] Paul Wagenseil. «*Hackers* Flood Epilepsy Web Forum with Flashing *Lights*». FoxNews.com, 31 de marzo de 2008; «Anonymous Attack Targets Epilepsy Sufferers». News.com.au, 1 de abril de 2008. <<

[21] Barnaby J. Feder. «A Heart Device Is Found Vulnerable to *Hacker* Attacks». En: *New York Times*, 12 de marzo de 2008; D. Halperin *et al*. «Pacemakers and Implantable Cardiac Defibrillators: *Software* Radio Attacks and Zero-Power Defenses». En: *IEEE Symposium on Security and Privacy*, *2008: SP 2008* (2008), págs. 129-142, doi:10.1109/ SP.2008.31. <<

[22] «Pacemaker *Hack* Can Deliver Deadly 830-Volt Jolt». En: *Computerworld*, 17 de octubre de 2012. <<

[23] «Dick Cheney Once Feared Terrorists Could Manipulate His Implanted Defibrillator to Induce Heart Attack». *Daily News* (edición de Nueva York), 19 de octubre de 2013. <<

[24] Jim Finkle. «Medtronic Probes Insulin Pump Risks». Reuters, 25 de octubre de 2011. <<

[25] «H*@cking* Implantable Medical Devices». Info-Sec Institute, acceso realizado el 4 de agosto de 2014, http:// resources.infosecinstitute.com/; Jordan Robertson. «*Hacker Shows Off* Lethal Attack by Controlling Wireless Medical Device». En: *Bloomberg*, 29 de febrero de 2012. <<

[26] Lauren Walker. «First Online Murder to Occur by End of 2014, Europol Warns». En: *Newsweek*, 6 de octubre de 2014. <<

[27] Laura Shin. «New Wireless Medical Device Swims Through Bloodstream». En: *Smart Planet*, 30 de junio de 2014. <<

[28] Marc Goodman. «Who Does the Autopsy? Criminal Implications of Implantable Medical Devices». Actas de la Segunda Conferencia USENIX sobre Salud, Seguridad y Privacidad, 8-12 de agosto de 2011, San Francisco, California. <<

[29] «The Pentagon’s Bionic Arm». CBS News, 12 de abril de 2009. <<

[30] «The Human Bionic Project: A Data Repository for Inspector Gadget *Body* Parts». En: *Co.Exist*, 26 de junio de 2013, fastcoexist.com. <<

[31] «“Bionic Pancreas” Astonishes Diabetes Researchers». NBC News, 13 de junio de 2014. <<

[32] Shaunacy Ferro. «Now You Can Control Someone Else's Arm over the Internet». En: *Popular Science*, 28 de mayo de 2013. <<

[33] «Global Biometrics Technology Market: Industry Analysis Size Share Growth Trends and Forecast, 2013-2019». KSWT, acceso realizado el 5 de agosto de 2014, http://www.kswt.com/. <<

[34] Junta Editorial. «Biometric Technology Takes *Off*». En: *New York Times*, 20 de septiembre de 2013. <<

[35] Rawlson King. «500 Million Biometric Sensors Projected for Internet of Things by 2018». En: *Biometric Update*, 31 de enero de 2014. <<

[36] Neal Ungerleider. «The Dark Side of Biometrics: 9 Million Israelis' Hacked Info Hits the Web». En: *Fast Company*, 24 de octubre de 2011. <<

[37] «Authorities Find Source That Leaked Every Israeli's Personal Information Online». Haaretz.com, 24 de octubre 2011. <<

[38] Larry Barrett. «30 Percent of Companies Will Use Biometric Identification by 2016». En: *ZDNet*, 4 de febrero de 2014. <<

[39] Andrew Moran. «990 Million Mobile Devices to Have Biometrics by 2017». En: *Examiner*, 9 de diciembre de 2013 <<

[40] «Galaxy S5 Fingerprint Sensor Hacked». BBC News, 16 de abril de 2014. <<

[41] Ms. Smith. «Laptop Fingerprint Reader Destroys “Entire Security Model of Windows Accounts”». En: *Network World*, 6 de septiembre de 2012. <<

[42] «Malaysia Car Thieves Steal Finger». BBC, 31 de marzo de 2005. <<

[43] «Biometric Fact and Fiction». *Economist*, 24 de octubre de 2002. <<

[44] Evan Blass. «*Play*-Doh Fingers Can Fool 90% of Scanners, Sez Clarkson U. Study». En: *Engadget*, 11 de diciembre de 2005. <<

[45] Kim Zetter. «*Hackers* Publish German Minister's Fingerprint». En: *Wired*, 31 de marzo de 2008; Cory Doctorow. «*Hackers* Publish Thousands of Copies of Fingerprint of German Minister Who Promotes Fingerprint Biometrics». En: *Boing Boing*, 1 de abril de 2008. <<

[46] Stuart Fox. «Chinese Woman Surgically Switches Fingerprints to Evade Japanese Immigration Officers». En: *Popular Science*, 8 de diciembre de 2009. <<

[47] «Japan “Fake Fingerprints” Arrest». BBC, 7 de diciembre de 2009 <<

[48] Kelly Jackson Higgins. «Black Hat Researcher *Hacks* Biometric System». En: *Dark Reading*, 31 de marzo de 2008. <<

[49] Mark Brown. «Japanese Billboard Recognises Age and Gender». En: *Wired UK*, 23 de septiembre de 2010. <<

[50] Natasha Singer. «When No One Is Just a Face in the Crowd». En: *New York Times*, 1 de febrero de 2014. <<

[51] Barbara De Lollis. «Houston Hilton Installs Facial Recognition». En: *USA Today*, 1 de octubre de 2010. <<

[52] «Biometric Surveillance Means Someone Is Always Watching». En: *Newsweek*, 17 de abril de 2014. <<

[53] Ibíd. <<

[54] Darren Murph. «Face.com Acquired by Facebook for an Estimated $80 Million+, Facial Tagging Clearly at the Forefront». En: *Engadget*, 18 de junio de 2012. <<

[55] Adam Clark Estes. «Facebook’s Doing Face Recognition Again and This Time America Doesn’t Seem to Mind». En: *Motherboard*, 5 de febrero 2013. <<

[56] Adi Robertson. «Facebook Users Have Uploaded a Quarter-Trillion Photos Since the Site's Launch». En: *Verge*, 17 de septiembre de 2013; «Biometrics and the Future of Identification». En: *NOVA Next*, acceso realizado el 6 de agosto de 2014. <<

[57] «How Spy Scandal Unravelled». BBC News, 7 de noviembre de 2013. <<

[58] James Risen and Laura Poitras. «N. S. A. Collecting Millions of Faces from Web Images». En: *New York Times*, 31 de mayo de 2014. <<

[59] Sebastian Anthony. «UK, the World's Most Surveilled State, Begins Using Automated Face Recognition to Catch Criminals». En: *ExtremeTech*, 17 de julio de 2014. <<

[60] Steve Henn. «9/11’s Effect on Tech». Marketplace.org, 8 de septiembre de 2011; Tim Greene. «Black Hat: System Links Your Face to Your Social Security Number and Other Private Things». En: *Network World*, 1 de agosto de 2011. <<

[61] Amir Efrati. «Google Acquires Facial Recognition Technology Company». En: *Digits* (blog), *Wall Street Journal*, 22 de julio de 2011; Kit Eaton. «How Google's New Face Recognition Tech Could Change the Web's Future». En: *Fast Company*, 25 de julio de 2011. <<

[62] Simson Garfinkel. «Google Glass Will Be a Huge Success-Unless People Find It Creepy». En: *MIT Technology Review*, 17 de febrero de 2014; Kashmir Hill. «Google Glass Facial Recognition App Draws Senator Franken's Ire». En: *Forbes*, 5 de febrero de 2014. <<

[63] Michelle Starr. «Facial Recognition App Matches Strangers to Online Profiles». En: *CNET*, 7 de enero de 2014. <<

[64] Jeremy Hsu. «FBI’s Facial Recognition Database Will Include Non-criminals». En: *IEEE Spectrum*, 16 de abril de 2014; Mark Rockwell. «Details Emerge on Scope of FBI’s Identification System». En: *FCW*, 15 de abril de 2014. <<

[65] Sara Reardon. «FBI Launches $1 Billion Face Recognition Project». En: *New Scientist*, 7 de septiembre de 2012. <<

[66] Adam Goldman. «More Than 1 Million People Are Listed in U. S. Terrorism Database». En: *Washington Post*, 5 de agosto de 2014; Consejo Editorial. «The Black Hole of Terrorism Watch Lists». En: *New York Times*, 15 de diciembre de 2013. <<

[67] John Leyden. «Laptop Facial Recognition Defeated by Photoshop». En: *Register*, 19 de febrero de 2009; Mark Saltzman. «FastAccess Anywhere: Face Recognition Replaces Password». En: *USA Today*, 4 de junio de 2013. <<

[68] Kim Zetter. «Reverse-Engineered Irises *Look* So Real, They Fool Eye-Scanners». En: *Wired*, 25 de julio de 2012. <<

[69] Noah Shachtman. «Army Tracking Plan: Drones That Never Forget a Face». En: *Wired*, 28 de septiembre de 2011. <<

[70] Stilgherrian. «Has Facebook Killed the Undercover Cop?». En: *CSO*, 25 de agosto de 2011. <<

[71] Neal Ungerleider. «Banks Are Deploying Voice Biometrics So That You Don’t Have to Tell Them Your Mother’s Maiden Name Again». En: *Fast Company*, 27 de mayo de 2014. <<

[72] Nick Anderson. «MOOCS-Here Come the Credentials». En: *College, Inc.* (blog), *Washington Post*, 9 de enero de 2013. <<

[73] Clint Boulton. «“*Post*-Password” Technology Verifies Users by Behavior». En: *Wall Street Journal*, 11 de julio de 2014. <<

[74] Rawlson King. «Biometric Research Note». Biometric Update, 21 de enero de 2013. <<

[75] Somini Sengupta. «Machines Made to Know You, by Touch, Voice, Even by Heart». En: *Bits* (blog), *New York Times*, 10 de septiembre de 2013. <<

[76] «NPL Takes Step Forward with Gait Recognition System». En: *Engineer*, 20 de septiembre de 2012. <<

[77] Christopher Mims. «Smart Phones That Know Their Users by How They Walk». En: *MIT Technology Review*, 16 de septiembre de 2010. <<

[78] Dieter Bohn. «Motorola *Shows Off* Insane Electronic Tattoo and Vitamin Authentication Prototype Wearables». En: *Verge*, 29 de mayo de 2013. <<

[79] Anthony. «UK, the World’s Most Surveilled State, Begins Using Automated Face Recognition to Catch Criminals». <<

[80] Para información adicional acerca de la realidad aumentada en lentes de contacto, *véase* Babak A. Parviz. «Augmented Reality in a Contact Lens». En: *IEEE Spectrum*, 1 de septiembre de 2009. <<

[81] Juniper Research. «Press Release: Over 2.5 Billion Mobile Augmented Reality Apps to Be Installed Per Annum by 2017», 29 de agosto de 2012. <<

[82] Luisa Rollenhagen. «Augmented Reality Catalog Places IKEA Furniture in Your Home». En: *Mashable*, 6 de agosto de 2013. <<

[83] Franziska Roesner, Tadayoshi Kohno y David Molnar. «Security and Privacy for Augmented Reality Systems». En: *Communications of the ACM* 57, n.º 4 (2014), págs. 88-96, doi:10.1145/2580723.2580730. <<

[84] Jane McGonigal, Conversación TED, http://www.ted.com/conversations/44/we_spend_3_billion _hours_a_wee.html; Jane McGonigal, *Reality Is Broken: Why Games Make Us Better and How They Can Change the World*. Nueva York: Penguin Books, 2011. <<

[85] Sarah Frier. «Facebook Makes $2 Billion Virtual Reality Bet with Oculus». En: *Bloomberg*, 26 de marzo de 2014. <<

[86] «Worlds Without End». *Economist*, 14 de diciembre de 2005. <<

[87] «A Korean Couple Let a *Baby* Die While They Played a Video Game». En: *Newsweek*, 27 de julio de 2014; «Korean Couple Let *Baby* Starve to Death While Caring for Virtual Child». En: *Telegraph*, 5 de marzo de 2010. <<

[88] «The Economy of Online Gaming Fraud Revealed: 3.4 Million Malware Attacks Every Day». En: *Kaspersky Lab*, 28 de septiembre de 2010. <<

[89] Carolyn Davis. «Virtual Justice: Online Game World Meets Real-World Cops and Courts». Philly.com, 8 de diciembre de 2010. <<

[90] Benjamin Duranske. «“Virtual Rape” Claim Brings Belgian Police to Second Life». En: *Virtually Blind*, 24 de abril de 2007. <<

[91] Anna Jane Grossman. «Single, White with Dildo». En: *Salon*, 30 de agosto de 2005. <<

[92] Sara Malm. «U. S. Intelligence Warned Terrorists Could Create Virtual Jihadist». En: *Mail Online*, 9 de enero de 2014. <<

[93] Mark Mazzetti y Justin Elliott. «Spies Infiltrate a Fantasy Realm of Online Games». En: *New York Times*, 9 de diciembre de 2013. <<

[94] James Ball. «Xbox Live Among Game Services Targeted by US and UK Spy Agencies». En: *Guardian*, 9 de diciembre de 2013; Ian Sherr. «Spy Game: NSA Said to Snoop on “World of Warcraft”». En: *Digits* (blog), *Wall Street Journal*, 9 de diciembre de 2013. <<

[95] Ibíd., Dan Costa. «This Is No Video Game». En: *PCMag*, 26 de septiembre de 2007. <<

[1] Agente especial Gary S. Cacace, declaración jurada, 28 de septiembre de 2011, http://www.justice.gov/; «Muslim Pleads Guilty to Plotting to Blow Up the Pentagon and Capitol with Model Airplanes Packed with Explosives». En: *Mail Online*, 20 de julio de 2012; «US Man Admits Model Plane Plot». BBC News; Brian Ballou. «Rezwan Ferdaus of Ashland Sentenced to 17 Years in Terror Plot; Plotted to Blow Up Pentagon, Capitol». Boston.com, 1 de noviembre de 2012; Jess Bidgood. «Rezwan Ferdaus of Massachusetts Gets 17 Years in Terrorist Plot». En: *New York Times*, 2 de noviembre de 2012. <<

[2] «Global Industrial Robotics Market Revenues to Surpass $37 Billion by 2018». En: *Business Wire*, 24 de febrero de 2014. <<

[3] Marcus Wohlsen. «Forget Robots. We’ll Soon Be Fusing Technology with Living Matter». En: *Wired*, 27 de mayo de 2014. <<

[4] Industrial Federation of Robotics, http://www.ifr.org/industrial-robots/statistics/. <<

[5] «Car, Airbag, Money: Robots Make Cars», vídeo, http://channel.nationalgeographic.com/; Tamara Walsh. «Rise of the Robots: 2 Industries Increasingly Turning to Robotics for Innovation». En: *Motley Fool*, 24 de agosto de 2014. <<

[6] Katie Lobosco. «Army of Robots to Invade Amazon Warehouses». En: *CNNMoney*, 22 de mayo de 2014. <<

[7] Rodney Brooks. «Robots at Work». World Future Society. En: *Futurist*, mayojunio de 2013. <<

[8] «The Invisible Unarmed». En: *Economist*, 29 de marzo de 2014. <<

[9] Stewart Pinkerton. «The Pros and Cons of Robotic Surgery». En: *Wall Street Journal*, 17 de noviembre de 2013. <<

[10] Jacques Marescaux *et al*. «Transcontinental Robot-Assisted Remote Telesurgery: Feasibility and Potential Applications». En: *Annals of Surgery* 235, n.º 4 (2002), págs. 300-301. <<

[11] Para obtener una panorámica definitiva del mundo de la robótica militar, *véase* la imprescindible obra de Peter W. Singer *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Nueva York: Penguin Books, 2009. <<

[12] Mitch Joel. «The Booming Business of Drones». En: *Harvard Business Review*, 4 de enero de 2013. <<

[13] Michael C. Horowitz. «The Looming Robotics Gap». *Foreign Policy*, 5 de mayo de 2014. <<

[14] Craig Whitlock. «Drone Strikes Killing More Civilians Than U. S. Admits». En: *Washington Post*, 22 de octubre de 2013. <<

[15] David Axe. «One in 50 Troops in Afghanistan Is a Robot». En: *Wired*, 7 de febrero de 2011; Sharon Gaudin. «U. S. Military May Have 10 Robots per Soldier by 2023». En: *Computerworld*, 14 de noviembre de 2013. <<

[16] Mark Prigg. «Google-Owned “Big Dog” Robot in First Live Trial with Marines». En: *Mail Online*, 14 de julio de 2014. <<

[17] «Cheetah Robot “Runs Faster Than Usain Bolt”». BBC News, 6 de septiembre de 2012; «March of the Robots». En: *Economist*, 2 de junio de 2012. <<

[18] «Rise of the Drones». En: *NOVA*, PBS, 23 de enero de 2013. <<

[19] Teal Group. «Teal Group Predicts Worldwide UAV Market Will Total $89 Billion». 17 de junio de 2013; Michael C. Horowitz. «The Looming Robotics Gap». En: *Foreign Policy*, 5 de mayo de 2014. <<

[20] Ratnesar Romesh. «Five Reasons Why Drones Are Here to Stay». En: *Bloomberg Businessweek*, 23 de mayo de 2013. <<

[21] «Rise of the Drones». <<

[22] John Markoff. «Google Puts Money on Robots, Using the Man Behind Android». En: *New York Times*, 4 de diciembre de 2013; Adam Clark Estes. «Meet Google's Robot Army. It's Growing». En: *Gizmodo*, 27 de enero de 2014. <<

[23] Bill Gates. «A Robot in Every Home». En: *Scientific American*, enero de 2007. <<

[24] *Véanse* el sitio web de iRobot: http://www.irobot.com/; el sitio web de Droplet: http://smartdroplet.com; el sitio web de Grillbot: http://grillbots.com, y Mark Prigg. «Forgotten to Feed the Dog? Don’t Panic, There’s an App for That (and It Will Even Tweet to Tell You How Much They’ve Eaten». En: *Mail Online*, 4 de junio de 2013. <<

[25] David McCormack. «“I Love My Drone”: Martha Stewart Shares Incredible Aerial Images of Her Estate as She Reveals Her Latest Must-Have Accessory for the Summer». En: *Mail Online*, 30 de julio de 2014. <<

[26] Marcelo Ballve. «The Market for Home Cleaning Robots Is Already Surprisingly Big, and There's Plenty of Room for Growth». En: *Business Insider*, 5 de junio de 2014. <<

[27] Erico Guizzo. «So, Where Are My Robot Servants?». En: *IEEE Spectrum*, 29 de mayo de 2014. <<

[28] Brandon Keim. «I, Nanny». En: *Wired*, 18 de diciembre de 2008. <<

[29] Mai Iida. «Robot Niche Expands in Senior Care». En: *Japan Times*, 19 de junio de 2013. <<

[30] Anne Tergesen y Miho Inada. «It’s Not a Stuffed Animal, It’s a $6,000 Medical Device». En: *Wall Street Journal*, 21 de junio de 2010. <<

[31] «Your *Alter Ego* on Wheels». En: *Economist*, 9 de marzo de 2013. <<

[32] Serene Fang. «Robot Care for Aging Parents». En: *Al Jazeera America*, 27 de febrero de 2014. <<

[33] Ryan Jaslow. «RP-VITA Robot on Wheels Lets Docs Treat Patients Remotely». CBS News, 19 de noviembre de 2013. <<

[34] «Robots Are the New Butlers at Starwood Hotels». CNBC, 12 de agosto de 2014. <<

[35] Carl Benedikt Frey y Michael A. Osborne. «The Future of Employment». Oxford Martin, 17 de septiembre de 2013, http://www.oxfordmartin.ox.ac.uk/. <<

[36] Para consultar un análisis excelente acerca del futuro de los robots, la automatización y el empleo, *véanse* Kevin Kelly. «Better Than Human: Why Robots Willand Must-Take Our Jobs». En: *Wired*, 24 de diciembre de 2012; Erik Brynjolfsson y Andrew McAfee. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. Nueva York: W. W. Norton, 2014. <<

[37] Francie Diep. «Associated Press Will Use Robots to Write Articles». En: *Popular Science*, 1 de julio de 2014. <<

[38] Paul Krugman. «Robots and Robber Barons». En: *New York Times*, 9 de diciembre de 2012. <<

[39] Lindsey Bever. «Seattle Woman *Spots* Drone Outside Her 26th-Floor Apartment Window, Feels “Violated”». En: *Washington Post*, 25 de junio de 2014. <<

[40] Rebecca J. Rosen. «So This Is How It Begins: Guy Refuses to *Stop* DroneSpying on Seattle Woman». En: *Atlantic*, 13 de mayo de 2013. Para consultar un análisis legal detallado sobre VANT y privacidad, *véase* John Villasenor. «Observations from Above: Unmanned Aircraft Systems and Privacy». En: *Harvard Journal of Law and Public Policy* 36, n.º 2 (primavera de 2013). <<

[41] Oficina Gubernamental de Contabilidad de Estados Unidos. *Unmanned Aircraft Systems*, septiembre de 2012, http://www.gao.gov/. <<

[42] Robert Langreth. «Unreported Robot Surgery Injuries Open Questions for FDA». En: *Bloomberg*, 29 de diciembre de 2013. <<

[43] «Surgical Robot da Vinci Scrutinized by FDA After Deaths, Other Surgical Nightmares». *Daily News* (edición de Nueva York), 9 de abril de 2013. <<

[44] «Robot Attacked Swedish Factory Worker». En: *Local*, 29 de abril de 2009. <<

[45] John Markoff y Claire Cain Miller. «As Robotics Advances, Worries of Killer Robots Rise». En: *New York Times*, 16 de junio de 2014. <<

[46] Gavin Knight. «March of the Terminators: But What Happens When Robot Warriors Turn Their Guns on Us?». En: *Mail Online*, 15 de marzo de 2009. <<

[47] Craig Whitlock. «When Drones Fall from the Sky». En: *Washington Post*, 20 de junio de 2014. <<

[48] Ibíd. <<

[49] «How Dangerous Could a Hacked Robot Possibly Be?». En: *Computerworld*, 8 de octubre de 2009. <<

[50] Siobhan Gorman, Yochi J. Dreazen, y August Cole. «Insurgents *Hack* U. S. Drones». En: *Wall Street Journal*, 18 de diciembre de 2009. <<

[51] Colin Lecher. «Texas Students Hijack a U. S. Government Drone in Midair». En: *Popular Science*, 28 de junio de 2012. <<

[52] John Roberts. «Drones Vulnerable to Terrorist Hijacking, Researchers Say». Fox News, 25 de junio de 2012. <<

[53] Scott Peterson y Payam Faramarzi. «Exclusive: Iran Hijacked US Drone, Says Iranian Engineer». En: *Christian Science Monitor*, 15 de diciembre de 2011. <<

[54] Noah Shachtman. «Exclusive: Computer Virus Hits U. S. Drone Fleet». En: *Wired*, 7 de octubre de 2011. <<

[55] Dan Goodin. «Flying *Hacker* Contraption Hunts Other Drones, Turns Them into Zombies». En: *Ars Technica*, 3 de diciembre de 2013. <<

[56] Andy Greenberg. «PIN-Punching Robot Can *Crack* Your Phone's Security Code in Less Than 24 Hours». En: *Forbes*, 22 de julio de 2013. <<

[57] «Drug Dealer Arrested in Spite of Home Robotic Protection: Police». En: *China Post*, 10 de agosto de 2014. <<

[58] Charlemagne. «Afghanistan-the Biggest Bomb Yet». Intel MSL, 15 de marzo de 2013, http://intelmsl.com/. <<

[59] Noah Shachtman. «Iraq Militants Brag: We’ve Got Robotic Weapons, Too». En: *Wired*, 4 de octubre de 2011. <<

[60] Harris. «FBI Warns Driverless Cars Could Be Used as “Lethal Weapons”». *Guardian*, 16 de julio de 2014. <<

[61] Jathan Sadowski. «Delivered by Drones: Are Tacocopters and Burrito Bombers the Next *Pony Express*?». En: *Slate*, 6 de agosto de 2013; Laura Stampler. «This Club Is Offering Poolside Drone Bottle Service». En: *Time*, 19 de junio de 2014. <<

[62] «Google Is Testing Delivery Drone System». En: *Wall Street Journal*, 29 de agosto de 2014. <<

[63] Sarah Zhang. «Drones That Aren’t Out to Kill You». En: *Mother Jones*, 6 de diciembre de 2012. <<

[64] «Canadian Mounties Claim First Person’s Life Saved by a Police Drone». En: *Verge*, 10 mayo de 2013. <<

[65] Andy Greenberg. «Flying Drone Can *Crack* Wi-Fi Networks, Snoop on Cell Phones». En: *Forbes*, 28 de julio de 2011. <<

[66] Spencer Ackerman. «Occupy the Skies! Protesters Could Use Spy Drones». En: *Wired*, 17 de noviembre de 2011. <<

[67] «Drone Is Caught Delivering Cocaine in Prison São Paulo Brazil». En: *Live Leak*, 10 de marzo de 2014; «Heroin by Helicopter.» En: *Voice of Russia*, 1 de febrero de 2011; Nick Evershed. «Drone Used in Attempt to Smuggle Drugs into Melbourne Prison, Say Police». En: *Guardian*, 10 de marzo de 2014; Mary-Ann Russon. «Drones Used to Deliver Drugs to Prisoners in Canada». En: *International Business Times*, 29 de noviembre de 2013; «Greece: Drone Drops Mobile Phones over Prison Walls». BBC News, 19 de agosto de 2014; «Crooks Get Creative to Smuggle Contraband». WALB News, 22 de noviembre de 2013. <<

[68] Meghan Neal. «Cartels Are Reportedly Building DIY Drones to Fly Drugs over the Border». En: *Motherboard*, 2 de junio de 2014; Doris Gómora. «Fabrican narcos sus propios drones, alerta la DEA». En: *El Universal*, 9 de julio de 2014. <<

[69] Mark Frauenfelder. «Man Arms DIY Drone with Paintball Handgun and Shoots Human Cardboard Cutouts». En: *Boing Boing*, 12 de diciembre de 2012. <<

[70] Colin Lecher. «Watch a Stun Gun Drone Tase an Intern». En: *Popular Science*, 7 de marzo de 2014. <<

[71] «R/C Helicopter with .45 Caliber Handgun». En: *Live Leak*, 10 de diciembre de 2008. <<

[72] Annalee Newitz. «This Video of a Drone with a Gun Will Freak You the Hell Out». En: *io9*, 14 de junio de 2013; «Viral Video Straps Colt .45 Handgun to a HomeUse Drone», comentarios. En: *Live Leak*, 18 de junio de 2013. <<

[73] Jason Koebler. «“Follow Me” Drones Will Hover by Your Side on a Digital “Leash”». En: *Motherboard*, 16 de junio de 2014. <<

[74] «RadioControlled Crop Dusting in Fukuoka», Japón, 2011, http://www.youtube.com/watch?v=N28KKb6i9hs. <<

[75] Sean Gallagher. «German Chancellor's Drone "Attack" *Shows* the Threat of Weaponized UAVs». En: *Ars Technica*, 18 de septiembre de 2013. <<

[76] Jon Fingas. «Near Collision with Airliner Prompts US to *Crack* Down on Drone Use». En: *Engadget*, 12 de mayo de 2014; Alwyn Scott. «U. S. Passenger *Jet* Nearly Collided with Drone in March». Reuters, 9 de mayo de 2014. <<

[77] John W. Whitehead. «Roaches, Mosquitoes, and Birds: The Coming MicroDrone Revolution». En: *Huffington Post*, 17 de abrilo de 2013. <<

[78] Tom Leonard. «US Accused of Making Insect Spy Robots». En: *Telegraph*, 10 de octubre de 2007. <<

[79] Whitehead. «Roaches, Mosquitoes, and Birds»; Emily Singer. «TR10: Biological Machines». En: *MIT Technology Review*, marzo/abril de 2009; Erico Guizzo. «Moth Pupa + MEMS Chip = Remote Controlled *Cyborg* Insect». En: *IEEE Spectrum*, 17 de febrero de 2009; Charles Q. Choi. «Military Developing Robot-Insect *Cyborgs*». NBC News, 14 de julio de 2009. <<

[80] Robert Lee Hotz. «Harvard Scientists Devise Robot Swarm That Can Work Together». En: *Wall Street Journal*, 15 de agosto de 2014. <<

[81] Jon Cartwright. «Rise of the Robots and the Future of War». En: *Guardian*, 20 de noviembre de 2010. <<

[82] Tim Hornyak. «Korean Machine-Gun Robots Start DMZ Duty». En: *CNET*, 14 de julio de 2010; Keith Wagstaff. «Future Tech? Autonomous Killer Robots Are Already Here». NBC News, 14 de mayo de 2014. <<

[83] Goldman Sachs. *2013 Annual Report*, http://www.goldmansachs.com/; Matt Clinch, «3-D Printing Market to Grow 500% in 5 Years». CNBC, 1 de abril de 2014. <<

[84] Jessica Leber. «This Man Thinks He Can 3-D Print an Entire House». En: *Co.Exist*, 12 de noviembre de 2013. <<

[85] Lyndsey Gilpin. «New 3D Bioprinter to Reproduce Human Organs, Change the Face of Healthcare». En: *Tech-Republic*, 1 de agosto de 2014; Melissa Davey. «3D Printed Organs Come a Step Closer». En: *Guardian*, 4 de julio de 2014; Kate Lyons. «Humans Could Be Fitted with Kidneys Made on 3D Printers». En: *Mail Online*, 23 de mayo de 2014. <<

[86] Ben Rooney. «The 3D Printer That Prints Itself». En: *Wall Street Journal*, 10 de junio de 2011; Brad Hart. «Will 3D Printing Change the World?». En: *Forbes*, 6 de marzo de 2012. <<

[87] Gartner. «Gartner Says Uses of 3D Printing Will Ignite Major Debate on Ethics and Regulation», Gartner.com, 29 de enero de 2014. <<

[88] Drew Prindle. «KeyMe Joins Forces with Shapeways to Bring You Custom 3D-Printed Key Copies». En: *Digital Trends*, 17 de diciembre de 2013. <<

[89] Ann Givens y Chris Glorioso. «New Technology Could Let Thieves Copy Keys». NBC New York, 21 de mayo de 2014. <<

[90] Andy Greenberg. «*Hacker* Opens High Security Handcuffs with 3D-Printed and Laser-Cut Keys». En: *Forbes*, 16 de julio de 2012. <<

[91] Tim Adams. «The “Chemputer” That Could Print Out Any Drug». En: *Guardian*, 21 de julio de 2012. <<

[92] Carole Cadwalladr. «Meet Cody Wilson, Creator of the 3D-Gun, Anarchist, Libertarian». *Guardian*, 8 de febrero de 2014. <<

[93] Andy Greenberg. «Here’s What It *Looks* Like to Fire a (Partly) 3D-Printed Gun». En: *Forbes*, 3 de diciembre de 2012. <<

[94] Andy Greenberg. «Meet the “Liberator”: Test-Firing the World’s First Fully 3D-Printed Gun». En: *Forbes*, 5 de mayo de 2013. <<

[95] Andy Greenberg. «How 3-D Printed Guns Evolved into Serious Weapons in Just One Year». En: *Wired*, 15 de mayo de 2014. <<

[96] Cheryl K. Chumley. «Israeli TV Crew Sneaks Printed 3-D Gun into KnessetTwice». En: *Washington Times*, 4 de julio de 2013. <<

[97] Greenberg. «How 3-D Printed Guns Evolved into Serious Weapons in Just One Year». <<

[98] Aliya Sternstein. «The FBI Is Getting Its Own, Personal 3D Printer for Studying Bombs». En: *Nextgov*, 13 de junio de 2014. <<

[1] Nina Golgowski. «“Syrian *Hackers*” Tweet FALSE Report of Explosions at White House and Send Panicked DOW Jones Plunging 100 Points». En: *Mail Online*, 23 de abril de 2013; Jim McTague. «Why High-Frequency Trading Doesn’t Compute». En: *Barron’s*, 11 de agosto de 2012; Shan Carter y Amanda Cox. «One 9/11 Tally». En: *New York Times*, 8 de septiembre de 2011; Doug Stanglin y David Jackson. «Timeline of AP Hacking, Reaction». En: *USA Today*, 23 de abril de 2013; Will Oremus. «Would You Click the Link in This *Email* That Apparently Tricked the AP». En: *Slate*, 23 de abril de 2013; Tom Lauricella, Kara Scanell y Jenny Strasburg. «How a Trading Algorithm Went Awry». En: *Wall Street Journal*, 2 de octubre de 2010; Bernard Condon. «*Stocks* Stumble After a Fake Tweet Announced White House Attack». Associated Press, 25 de abril de 2013; Nick Baumann. «Too Fast to Fail: Is High-Speed Trading the Next Wall Street Disaster?». En: *Mother Jones*, enero-febrero de 2013. <<

[2] Vinod Khosla. «Do We Need Doctors or Algorithms?». En: *TechCrunch*, 10 de enero de 2012. <<

[3] Rachael King. «Artificial Intelligence May Reduce Soaring E-discovery Costs». En: *CIO Journal*, 29 de octubre de 2013. <<

[4] Amy Biegelsen. «Unregulated FICO Has Key Role in Each American’s Access to Credit». Center for Public Integrity, 17 de mayo de 2011. <<

[5] Adam D. I. Kramer, Jamie E. Guillory y Jeffrey T. Hancock. «Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks». En: *Proceedings of the National Academy of Sciences* 111, n.º 24 (2014): 8788-90, doi:10.1073/ pnas.1320040111. <<

[6] Reed Albergotti y Elizabeth Dwoskin. «Facebook Study Sparks *Soul*-Searching and Ethical Questions». En: *Wall Street Journal*, 30 de junio de 2014. <<

[7] Kashmir Hill. «Facebook Added “Research” to User Agreement 4 Months After Emotion Manipulation Study». En: *Forbes*, 30 de junio de 2014; Michelle N. Meyer. «Everything You Need to Know About Facebook’s Controversial Emotion Experiment». En: *Wired*, 30 de junio de 2014. <<

[8] Gabriel Hallevy. «The Criminal Liability of Artificial Intelligence Entities». Documento académico de la Social Science Research Network, 15 de febrero de 2010, http://papers.ssrn.com/. <<

[9] Chris Greenwood. «Will Russia Hand Over Man Behind the Gameover Zeus Ransom Virus? FBI Issues Warrant for $100M Cybercrime Mastermind». En: *Mail Online*, 2 de junio de 2014. <<

[10] McAfee, Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime*, junio de 2014. <<

[11] Jenny Awford. «Student Accused of Murder “Asked Siri Where to Hide *Body*”, Say Police». En: *Mail Online*, 13 de agosto de 2014. <<

[12] «IBM Watson». Sitio web de IBM, http://www-03.ibm.com/press/us/en/presskit/27297.wss. <<

[13] «IBM Watson Hard at Work». Memorial Sloan Kettering Cancer Center, 8 de febrero de 2013; Larry Greenemeier. «Will IBM's Watson Usher in a New Era of Cognitive Computing». En: *Scientific American*, 13 de noviembre de 2013. <<

[14] Ray Kurzweil. *The Singularity Is Near: When Humans Transcend Biology*. Nueva York: Penguin Books, 2006, pág. 7. <<

[15] Catherine Shu. «Google Acquires Artificial Intelligence Startup DeepMind». En: *TechCrunch*, 26 de enero de 2014. <<

[16] Stephen Hawking *et al*. «Stephen Hawking: “Transcendence *Looks* at the Implications of Artificial Intelligence-but Are We Taking AI Seriously Enough?”». En: *Independent*, 1 de mayo de 2014. <<

[17] Reed Albergotti. «Zuckerberg, Musk Invest in Artificial Intelligence Company». En: *Wall Street Journal*, 21 de marzo de 2014. <<

[18] «Brain Research Through Advancing Innovative Neurotechnologies», 25 de agosto de 2014, http://www.nih.gov/science/brain/; Susan Young Rojahn. «The BRAIN Project Will Develop New Technologies to Understand the Brain». En: *MIT Technology Review*, 8 de abril de 2013. <<

[19] Priya Ganapati. «Cognitive Computing Project Aims to Reverse-Engineer the Mind». En: *Wired*, 6 de febrero de 2009; Vincent James. «Chinese Supercomputer Retains “World’s Fastest” Title, Beating US and Japanese Competition». En: *Independent*, 19 de noviembre de 2013. <<

[20] Ray Kurzweil. *How to Create a Mind: The Secret of Human Thought Revealed*. Nueva York: Penguin Books, 2013; Michio Kaku. *El futuro de nuestra mente: el reto científico para entender, mejorar y fortalecer nuestra mente*. Barcelona: Debate, 2014. <<

[21] Joseph Brean. «Build a Better Brain». En: *National Post*, 31 de marzo de 2012; Cade Metz. «IBM Dreams Impossible Dream». En: *Wired*, 9 de agosto de 2013. <<

[22] Kaku, *El futuro de nuestra mente*. <<

[23] Peter Clarke. «IBM Seeks Customers for Neural Network Breakthrough». En: *Electronics360*, 7 de agosto de 2014. <<

[24] Paul A. Merolla *et al*. «A Million Spiking-Neuron Integrated Circuit with a Scalable Communication Network and Interface». En: *Science*, 8 de agosto de 2014, págs. 668-673, doi:10.1126/science.1254642; Robert F. Service. «The Brain Chip». En: *Science*, 8 de agosto de 2014, págs. 614-616, doi:10.1126/science.345.6197.614; John Markoff. «IBM Develops a New Chip That Functions Like a Brain». En: *New York Times*, 7 de agosto de 2014. <<

[25] Ray Kurzweil. «The Coming Merging of Mind and Machine». En: *Scientific American* 18 (2008), págs. 20-25, doi:10.1038/scientificamerican0208-20sp. <<

[26] Gary Marcus y Christof Koch. «The Future of Brain Implants». En: *Wall Street Journal*, 14 de marzo de 2014. <<

[27] Leigh R. Hochberg *et al*. «Reach and Grasp by People with Tetraplegia Using a Neurally Controlled Robotic Arm». En: *Nature*, 17 de mayo de 2012, 372-75, doi:10.1038/nature11076. <<

[28] Robert McMillan. «This Guy Just Built a Mind-Controlled Robot». En: *Wired*, 22 de agosto de 2014. <<

[29] Dave Lee. «Google Glass *Hack* Allows Brainwave Control». BBC News, 9 de julio de 2014; Ingrid Lunden. «Forget “OK Glass”, MindRDR Is a Google Glass App You Control with Your Thoughts». En: *TechCrunch*, 9 de julio de 2014. <<

[30] Sebastian Anthony. «First Human Brain-to-Brain Interface Allows Remote Control over the Internet, Telepathy Coming Soon». En: *ExtremeTech*, 28 de agosto de 2013. <<

[31] Alan S. Cowen, Marvin M. Chun y Brice A. Kuhl. «Neural Portraits of Perception: Reconstructing Face Images from Evoked Brain Activity». En *NeuroImage*, próxima publicación, http://camplab.psych.yale.edu/; Mark Prigg. «Mind Reading Experiment Reconstructs Faces from Brain Scans». En: *Mail Online*, 28 de marzo de 2014. <<

[32] «How Technology May Soon “Read” Your Mind». CBS News, 4 de enero de 2009. <<

[33] IBM Research. «Mind Reading Is No Longer Science Fiction», 19 de diciembre de 2011, http://ibmresearchnews.blogspot.com/. <<

[34] Mark Harris. «MRI Lie Detectors». En: *IEEE Spectrum*, 30 de julio de 2010. <<

[35] Adi Narayan. «The fMRI Brain Scan: A Better Lie Detector?». En: *Time*, 20 de julio de 2009. <<

[36] Anand Giridharadas. «India’s Novel Use of Brain Scans in Courts Is Debated». En: *New York Times*, 15 de septiembre 2008; Angela Saini. «The Brain Police: Judging Murder with an MRI». En: *Wired UK*, 27 de mayo de 2009. <<

[37] Geeta Dayal. «Researchers *Hack* Brainwaves to Reveal PINs, Other Personal Data». En: *Wired*, 29 de agosto de 2012. <<

[38] Erika Check Hayden. «Company Claims to Have Sequenced Man's Genome Cheaply». En: *Nature News*, 8 de febrero de 2008, doi:10.1038/news.2008.563. <<

[39] Mike Orcutt. «Bases to *Bytes*». En: *MIT Technology Review*, 25 de abril de 2012; Matthew Herper. «DNA Sequencing: Beating Moore's Law Since January 2008». En: *Forbes*, 13 de mayo de 2011. <<

[40] Erika Check Hayden. «Technology: The $1,000 Genome». En: *Nature*, 19 de marzo de 2014, págs. 294-295, doi:10.1038/507294a; Ashlee Vance. «Human Gene Mapping Price to Drop to $1,000, Illumina Says». En: *Bloomberg*, 15 de enero de 2014. <<

[41] Jon Mooallem. «Do-It-Yourself Genetic Engineering». En: *New York Times Magazine*, 14 de febrero de 2010; Jack Hitt. «Guess What's Cooking in the Garage». En: *Popular Science*, 31 de mayo de 2012. <<

[42] Zoë Corbyn. «Craig Venter: “This Isn’t a Fantasy *Look* at the Future. We Are Doing the Future”». En: *Guardian*, 12 de octubre de 2013. <<

[43] Lisa M. Krieger. «Biological Computer Created at Stanford». En: *San Jose Mercury News*, 29 de marzo de 2013; Tim Requarth y Greg Wayne. «Tiny Biocomputers Move Closer to Reality». En: *Scientific American*, 2 de noviembre de 2011; Adam Baer. «Why Living Cells Are the Future of Data Processing». En: *Popular Science*, 5 de noviembre de 2012. <<

[44] Clay Dillow. «Biostorage Scheme Turns E. coli Bacteria into Hard Drives». En: *Popular Science*, 10 de enero de 2011. <<

[45] Wyss Institute. «Writing the Book in DNA», 16 de agosto de 2012, http://wyss.harvard.edu/viewpressrelease/93/. <<

[46] *Ibíd.* <<

[47] Chiropractic Resource Organization. «NIH Heads Foresee the Future», http://www.chiro.org/; Helen Thomson. «Deaf People Get Gene Tweak to Restore Natural Hearing». En: *New Scientist,* 23 de abril de 2014. <<

[48] George M. Church. *Regenesis: How Synthetic Biology Will Reinvent Nature and Ourselves. Nueva* York: Basic Books, 2012; J. Craig Venter. *Life at the Speed of Light: From the Double Helix to the Dawn of Digital Life*. Nueva York: Viking Adult, 2013. <<

[49] Kim-Mai Cutler. «Glowing Plant Is One of Y Combinator’s Very First Biotech Startups». En: *TechCrunch*, 11 de agosto 2014. <<

[50] Rebecca Skloot. *La vida inmortal de Henrietta Lacks*. Madrid: Temas de Hoy, 2011; *Moore v. Regents of University of California* (1990) 51 Cal. 3d 120 (271 Cal. Rptr. 146, 793 P.2d 479), Justia Law, acceso realizado el 12 de septiembre de 2014, http:// law.justia.com/. <<

[51] A case of *Moore v. Regents of the University of California*. El 9 de julio de 1990, el tribunal determinó que el tejido y las células descartados de una persona no son de su propiedad y, por consiguiente, pueden comercializarse. <<

[52] James Randerson. «What DNA Can Tell Us». En: *Guardian*, 26 de abril de 2008. <<

[53] Ian Sample. «Male Sexual Orientation Influenced by Genes, Study *Shows*». En: *Guardian*, 13 de febrero de 2014; Patricia Cohen. «Genetics and Crime at Institute of Justice Conference». En: *New York Times*, 19 de junio de 2011. <<

[54] National Human Genome Research Institute, Genetic Information Nondiscrimination Act of 2008, http:// www.genome.gov/; National Human Genome Research Institute. «Genetic Discrimination», http://www.genome.gov/. <<

[55] Adam Cohen. «Can You Be Fired for Your Genes?». En: *Time*, 20 de febrero de 2012. <<

[56] Statens Serum Institut. «The Danish Neonatal Screening Biobank», http://www.ssi.dk. <<

[57] Andrew Pollack. «DNA Evidence Can Be Fabricated, Scientists *Show*». En: *New York Times*, 18 de agosto de 2009; Dan Frumkin *et al*. «Authentication of Forensic DNA Samples». En: *Forensic Science International: Genetics* 4, n.º 2 (2010): págs. 95-103, doi:10.1016/j.fsigen.2009.06.009. <<

[58] Fiona Macrae. «DNA Evidence Can Be Fabricated and Planted at Crime Scenes, Scientists Warn». En: *Mail Online*, 19 de agosto de 2009. <<

[59] Sharon Begley. «Citing Privacy Concerns, U. S. Panel Urges End to Secret DNA Testing». Reuters, 11 de octubre de 2012. <<

[60] Erin Carlyle. «Billionaire Druglords». En: *Forbes*, 13 de marzo de 2012. <<

[61] Bijan Stephen. «Pablo Escobar’s Hippos Are Running Wild in Colombia». En: *Time*, 28 de junio de 2014. <<

[62] Jeremy McDermott. «Drug Lords Develop High-Yield Coca Plant». En: *Telegraph*, 27 de agosto de 2004; Goodman. «What Business Can Learn from Organized Crime». <<

[63] Marc Goodman. «A Vision for Crimes in the Future». Conferencia TED Talk, julio de 2012. <<

[64] «Bakterien können ohne viel Aufwand Cannabis-Wirkstoff produzieren», derStandard.at, 17 de agosto de 2010, http://derstandard.at/; Luc Henry. «Instead of Poppies, Engineering Microbes». En: *Discover*, 9 de septiembre de 2014; «A New Opium Pipe». En: *Economist*, 30 de agosto de 2014. <<

[65] Joel O. Wertheim. «The Re-emergence of H1N1 Influenza Virus in 1977: A Cautionary Tale for Estimating Divergence Times Using Biologically Unrealistic Sampling Dates». En: *PLoS ONE* 5, n.º 6 (2010): e11184, doi:10.1371/journal, pone.0011184. <<

[66] Alison Young. «Vial of Deadly Virus Missing at Texas Bioterror Laboratory». En: *USA Today*, 25 de marzo de 2013; «Paris LaboratoryLosesDeadlySARSVirus Samples». France24, 16 de abril de 2014. <<

[67] Eric Schmitt y Thom Shanker. «Qaeda Trying to Harness Toxin, Ricin, for Bombs, U. S. Says». En: *New York Times*, 12 de agosto de 2011. <<

[68] Marc Goodman. «The Bio-crime Prophecy». En: *Wired*, 28 de mayo de 2013. <<

[69] Erika Check. «Poliovirus Advance Sparks Fears of Data Curbs». En: *Nature*, 18 de julio de 2002, págs. 265, doi:10.1038/418265a. <<

[70] Masaki Imai et *al*. «Experimental Adaptation of an Influenza H5 HA Confers Respiratory Droplet Transmission to a Reassortant H5 HA/H1N1 Virus in Ferrets». En: *Nature*, 2 de mayo de 2012, doi:10.1038/nature10831; Bryan Walsh. «Should Journals Describe How Scientists Made a Killer Flu?». En: *Time*, 21 de diciembre de 2011. <<

[71] Denise Grady y William J. Broad. «U. S. Asks Journals to Censor Articles on Bird Flu Virus». En: *New York Times*, 20 de diciembre de 2011. <<

[72] Andrew Hessel, Marc Goodman y Steven Kotler. «Hacking the President's DNA». En: *Atlantic*, 24 de octubre de 2013. <<

[73] Robert Booth and Julian Borger. «US Diplomats Spied on UN Leadership». En: *Guardian*, 28 de noviembre de 2010; Spencer Ackerman. «U. S. Chases Foreign Leaders' DNA, WikiLeaks *Shows*». En: *Wired*, 29 de noviembre de 2010. <<

[74] Marcelo Soares. «The Great Brazilian Sat-*Hack* Crackdown». En: *Wired*, 20 de abril de 2009. <<

[75] Ellie Zolfagharifard. «Incredible Image *Shows* How Earth Is Entirely Surrounded by Junk». En: *Mail Online*, 13 de diciembre de 2013. <<

[76] William J. Broad y David E. Sanger. «China Tests Anti-satellite Weapon, Unnerving U. S.». En: *New York Times*, 18 de enero de 2007. <<

[77] Joey Cheng. «Critical Military Satellite Systems Are Vulnerable to Hacking». En: *Defense Systems*, 23 de abril de 2014 <<

[78] Tony Capaccio y Jeff Bliss. «Chinese Military Suspected in *Hacker* Attacks on U. S. Satellites». En: *Bloomberg*, 26 de octubre de 2011. <<

[79] Samuel Gibbs. «International Space Station Attacked by “Virus Epidemics”.» En: *Guardian*, 12 de noviembre de 2013. <<

[80] Ellie Zolfagharifard. «Cosmonaut Accidentally Infected the ISS with a Virus on a USB Stick». En: *Mail Online*, 12 de noviembre de 2013; «Cosmonaut Carries Computer Virus Aboard International Space Station». En: *PBS News-Hour*, 11 de noviembre de 2013. <<

[81] Damien Francis. «Computer Virus Infects Orbiting Space Station». En: *Guardian*, 27 de agosto de 2008. <<

[82] David Meyer. «*Hackers* Plan Space Satellites to Combat Censorship». BBC News, 4 de enero de 2012. <<

[83] «Graphene “Made with Kitchen Blender”». BBC News, 22 de abril de 2014; David Larousserie. «Graphene-the New Wonder Material». En: *Guardian*, 22 de noviembre de 2013. <<

[84] Nancy S. Giges. «Top 5 Trends in Nanotechnology». ASME, marzo de 2013. <<

[85] «How Stuff Works “Nanotechnology Cancer Treatments”». En: *HowStuffWorks*, acceso realizado el 14 de septiembre de 2014, http://health.howstuffworks.com; Dean Ho. «Fighting Cancer with Nanomedicine». En: *Scientist*, 1 de abril de 2014. <<

[86] John Gehl. «Nanotechnology: Designs for the Future». En: *Ubiquity*, julio de 2000, http://ubiquity.acm.org/. <<

[87] «Modern Marvels: Doomsday Tech DVD». History Channel, 28 de diciembre de 2004. <<

[88] Eric Drexler. *Engines of Creation: The Coming Era of Nanotech-nology*. Garden City, Nueva York: Anchor, 1987), cap. 4. <<

[89] Robert A. Freitas Jr. «The Gray Goo Problem». En: *Kurzweil Accelerating Intelligence*, 20 de marzo de 2001; «Address Nanotechnology Concerns, Experts Urge». Reuters, 15 de noviembre de 2006. <<

[90] Paul Rincon. «Nanotech Guru Turns Back on Goo». BBC, 9 de junio de 2004. <<

[91] Jacob Aron. «Google’s Quantum Computer Flunks Landmark Speed Test». En: *New Scientist*, 15 de enero de 2014. <<

[92] Nick Statt. «Confirmed, Finally, D-Wave Quantum Computer Is Sometimes Sluggish». En: *CNET*, 19 de junio de 2014. <<

[93] Tom Simonite. «The CIA and Jeff Bezos Bet on Quantum Computing». En: *MIT Technology Review*, 4 de octubre de 2012. <<

[94] Ibíd. <<

[95] Mohit Arora. «How Secure Is AES Against Brute Force Attacks?». En: *EETimes*, May 7, 2012. <<

[96] Steven Rich y Barton Gellman. «NSA Seeks to Build Quantum Computer That Could *Crack* Most Types of Encryption». En: *Washington Post*, 2 de enero de 2014; «Quantum Computing, the NSA, and the Future of Cryptography». En: *On Point with Tom Ashbrook*, WBUR. <<

[97] Bill Joy. «Why the Future Doesn’t Need Us». En *Wired*, abril de 2000. <<

[1] Melanie Pinola. «F**k It, Ship It». En: *Lifehacker*, 14 de agosto de 2012. <<

[2] Para consultar un análisis excelente de los desafíos a la seguridad que plantea el código del *software* inseguro *véase* el artículo de Quinn Norton «Everything Is Broken» en https://medium.com/. <<

[3] «Be Still My Breaking Heart». *Dan Kaminsky's Blog*. <<

[4] Leah Hoffmann. «Risky Business». En: *Communications of the ACM* 54, n.º 11 (2011): 20, doi:10.1145 /2018396.2018404. <<

[5] First Research. «Computer *Software* Industry Profile», 25 de agosto de 2014. <<

[6] Jane Chong. «Bad Code: Should *Software* Makers Pay? (Part 1)». En: *New Republic*, 3 de octubre de 2013. <<

[7] «Achievements in Public Health, 1900-1999 Motor Vehicle Safety». En: *Morbidity and Mortality Weekly Report*, 14 de mayo de 1999, http://www.cdc.gov/. <<

[8] Alex Wilhelm. «Facebook Sets Revenue per User Records Around the World in Q2». En: *TechCrunch*, 23 de julio de 2014. <<

[9] Ethan Zuckerman. «The Internet's Original Sin». En: *Atlantic*, 14 de agosto de 2014. <<

[10] Graham Cluley. «55% of Net Users Use the Same Password for Most, If Not All, Websites». En: *Naked Security*, 23 de abril de 2013; «39 Percent of Smart Phone Users Don’t Secure Their Phones». En: *Consumer Reports News*, 1 de mayo de 2013. <<

[11] Deloitte. «2013 Technology Predictions», 2013, http://www.deloitte.com. <<

[12] HP. «HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack», 29 de julio de 2014. <<

[13] Ben Elgin, Michael Riley y Dune Lawrence. «Former Home Depot Managers Depict “C-Level” Security Before the *Hack*». En: *Bloomberg Businessweek*, 12 de septiembre de 2014. <<

[14] IBM Managed Security Services. «2014 Cyber Security Intelligence Index». 22 de julio de 2014; Fran Howarth. «The Role of Human Error in Successful Security Attacks». En: *Security Intelligence*, 2 de septiembre de 2014. <<

[15] «Computer Immune Systems». Departamento de Ciencia Informática, Universidad de Nuevo México, http://www.cs.unm.edu. <<

[16] Larry Greenemeier. «*Software* Mimics Ant Behavior by Swarming Against Cyber Threats». En: *Observations* (blog), *Scientific American*, 28 de septiembre de 2009. <<

[17] Mike Masnick. «DHS Boss, in Charge of Cybersecurity, Doesn’t Use *Email* or Any Online Services». En: *Techdirt*, 28 de septiembre de 2012. <<

[18] Michelle R. Smith, «Kagan: Court Hasn’t Really “Gotten to” *Email*». En: *Big Story*, 20 de agosto de 2013. <<

[19] Departamento de Defensa del Gobierno australiano, «Top 4 Mitigation Strategies to Protect Your ICT System», http://www.asd.gov.au/; Departamento de Defensa del Gobierno australiano, «The Cyber Threat», http://www.asd.gov.au/. <<

[20] Verizon RISK Team. «2012 Data Breach Investigations Report 3», acceso realizado a través de *Wired*. <<

[21] Karl Frederick Rauscher. «The Internet Health Model for Cybersecurity». EastWest Institute, 2 de junio de 2012. <<

[1] David Weinberg. «95 Percent of U. S. ATMs Run on Windows XP». MarketPlace.org, 19 de marzo de 2014. <<

[2] Jeffrey M. Jones. «Congress Job Approval Starts 2014 at 13%». Gallup, 14 de enero de 2014. <<

[3] Estrategia de la Casa Blanca para la Seguridad Nacional, octubre de 2007, página 4, http://www.dhs.gov/xlibrary/assets/nat _strat_homelandsecurity_2007.pdf. <<

[4] *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, 15 de julio de 2010, http://www.gao.gov/. <<

[5] «Mexico’s Drug War: 50,000 Dead in Six Years». En: *Atlantic*, 17 de mayo de 2012; Sara Ines Calderon. «In Mexico, Tech Is Used to Help Combat Narco Violence, Insecurity». En *TechCrunch*, 25 de diciembre de 2012; Michele Coscia. «How and Where Do Criminals Operate? Using Google to Track Mexican Drug Trafficking Organizations». Harvard Kennedy School, 23 de octubre de 2012. <<

[6] George Arnett y James Ball. «Are UK MPs Really Claiming More Expenses Now Than Before the Scandal?». En: *Guardian*, 12 de septiembre de 2014; Michael Anderson. «Four Crowdsourcing Lessons from the Guardian's (Spectacular) ExpensesScandal Experiment». Nieman Lab, 23 de junio de 2009. <<

[7] «Shortage of Cybersecurity Professionals Poses Risk to National Security», junio de 2014, http://www.rand.org/news/press/2014/06/18.html. <<

[8] Cisco. *Cisco 2014 Annual Security Report*; Lewis Morgan. «Global Shortage of Two Million Cyber Security Professionals by 2017». En: *IT Governance*, 30 de octubre de 2014, http://www.itgovernance.co.uk/. <<

[9] Ellen Nakashima. «Cybersecurity Should Be More Active, Officials Say». En: *Washington Post*, 16 de septiembre de 2012. <<

[10] «University Professor Helps FBI *Crack* $70 Million Cybercrime *Ring*». En: *Rock Center with Brian Williams*, 21 de marzo de 2012. <<

[11] Ben Rooney. «U. K. Government Says It Can’t Tackle Cybercrime on Its Own». En: *Wall Street Journal*, 25 de noviembre de 2011. <<

[12] Jane McGonigal. «We Spend 3 Billion Hours a Week as a Planet Playing Videogames. Is It Worth It? How Could It Be MORE Worth It?». Conversaciones TED, http:// www.ted.com/. <<

[13] Miguel Angel Luengo-Oroz, Asier Arran y John Frean. «Crowdsourcing Malaria Parasite Quantification». En: *Journal of Medical Internet Research*, 29 de noviembre de 2012. <<

[14] Katia Moskvitch. «Online Game Foldit Helps Anti-AIDS Drug Quest». BBC News, 20 de septiembre de 2011, http://www.bbc.com/news/technology-14986013; Matt Peckham. «Foldit Gamers Solve AIDS *Puzzle* That Baffled Scientists for a Decade». En: *Time*, 19 de septiembre de 2011. <<

[1] De acuerdo con un estudio realizado por el Departamento de Defensa australiano, http://www.asd.gov.au/publications/Catch_Patch_Match.pdf. <<

[*] La Línea Maginot fue una línea de defensa que Francia construyó a lo largo de su frontera con Alemania tras la Primera Guerra Mundial. Debido a un error estratégico, la línea no evitó la derrota de Francia al estallar la Segunda Guerra Mundial en 1940. Los franceses basaron su estrategia en su experiencia de la guerra de trincheras, que había forjado un paradigma bélico de grandes frentes de batalla estáticos. Pero la introducción de nuevos elementos en escena, como unidades acorazadas o aviones de guerra, hicieron que la línea Maginot pasase a la historia como uno de los fracasos estratégicos más costosos e inútiles. (*N. de la T.*) <<

[*] Snapchat es una aplicación móvil que permite el envío de fotos que se «destruyen» entre uno y diez segundos después de su recepción. La aplicación permite a los usuarios tomar fotografías, grabar vídeos, añadir textos y dibujos y mandarlos a una lista de contactos limitada. Estos vídeos y fotografías se conocen como «Snaps», y los usuarios pueden controlar el tiempo por el que éstos serán visibles (de 1 a 10 segundos de duración), tras lo cual desaparecerán de la pantalla del destinatario y serán borrados del servidor de Snapchat. (*N. de la T.*) <<

[*] *Script kiddie*: anglicismo que designa a una persona falta de habilidades técnicas, sociabilidad o madurez que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender. Es un término despectivo utilizado para describir a aquellos que utilizan programas y *scripts* desarrollados por otros para atacar sistemas de computadoras y redes. (*N. de la T.*) <<

[*] *Phreakers*: anglicismo que designa a una persona que se dedica a estudiar el funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, compañías telefónicas, sistemas que componen una red telefónica y electrónica aplicada a sistemas telefónicos y pueden llegar a realizar actividades no autorizadas con los teléfonos, por lo general móviles. (*N. de la T.*) <<

[*] El *phishing* o suplantación de la identidad designa una estrategia informática que consiste en intentar adquirir información confidencial (como una contraseña, datos de una tarjeta de crédito o información bancaria) de forma fraudulenta. El cibercriminal se hace pasar por una empresa de confianza en una aparente comunicación oficial electrónica, por lo general un mensaje de correo electrónico. (*N. de la T.*) <<

[*] Un préstamo o crédito fácil (también llamado «préstamo personal», «crédito rápido» o «dinero directo») es un préstamo por una cantidad reducida y a corto plazo cuya devolución acostumbra a estar relacionada con el día en que el solicitante cobra la nómina, si bien éste no es un requisito obligatorio. (*N. de la T.*) <<

[*] Facebook/¿Libro del odio? (*N. de la T.*) <<

[*] El término *botnet* designa una red de robots *informáticos* o bots, que se ejecutan de manera autónoma y automática. El creador de la botnet controla los ordenadores y servidores infectados de forma remota. Este tipo de redes se utilizan con fines delictivos. (*N. de la T.*) <<

[*] El término *astroturfing* describe campañas de relaciones públicas enmarcadas en la propaganda electoral y los anuncios comerciales que pretenden transmitir una impresión de espontaneidad provocada por relación con el entorno social. (*N. de la T.*) <<

[*] Mecanismos de piramidación mediante la adquisición de acciones de compañías para inflar su valor comercial real y posteriormente venderlas para obtener ganancias antes de que su precio se desplome en las bolsas de valores. (*N. de la T.*) <<

[*] Operación Voz Sincera. (*N. de la T.*) <<

[*] Peter Ferdinand Drucker (1909-2005), abogado y tratadista austríaco, es considerado el mayor filósofo de la administración del siglo XX. Autor de 35 libros, sus ideas fueron decisivas en la configuración de la «empresa moderna». (*N. de la T.*) <<

[*] El *freemium* (contracción de «free» y «*premium*») es un modelo de negocio que ofrece servicios básicos gratuitos, y cobra los más avanzados o especiales. Este modelo ha ganado popularidad con su uso por parte de las empresas relacionadas con la Web 2.0. (*N. de la T.*) <<

[*] Los Campos Elíseos son una sección paradisíaca del Hades o Inframundo, el lugar donde las «sombras» (almas inmortales) de los hombres virtuosos y los guerreros heroicos pasarán la eternidad en una existencia dichosa y feliz. (*N. de la T.*) <<

[*] Martha Helen Kostyra, más conocida como Martha Stewart, es una empresaria, escritora y presentadora de televisión estadounidense que ha logrado construirse un imperio mediático con su negocio de estilo de vida y cocina. (*N. de la T.*) <<

[*] Sistema global para comunicaciones móviles. (*N. de la T.*) <<

[*] John Joseph Gotti (1940-2002), fue un importante capo de la mafia estadounidense. (*N. de la T.*) <<

[*] En el original, *white hat hackers*, piratas informáticos que se oponen al uso del *spam*. (*N. de la T.*) <<

[*] Proyecto para la denuncia de la corrupción y la delincuencia organizada. (*N. de la T.*) <<

[*] En español, la Promesa de Donar, una campaña filantrópica lanzada en 2010 por Warren Buffet y Bill Gates, cuyo fin es, según define en su página web, «invitar a las personas y familias más adineradas de América a que se comprometan a donar la mayor parte de su fortuna con fines filantrópicos». (*N. de la T.*) <<

[*] El Proyecto Manhattan fue un proyecto científico acometido durante la Segunda Guerra Mundial por Estados Unidos en colaboración con el Reino Unido y Canadá con el objetivo de crear la primera bomba atómica antes que la Alemania nazi. (*N. de la T.*) <<

[*] Conjunto de universidades estadounidenses que tienen en común unas connotaciones académicas de excelencia y de elitismo por su antigüedad y admisión selectiva. También se las conoce como «las ocho antiguas» o «las Hiedras». (*N. de la T.*) <<