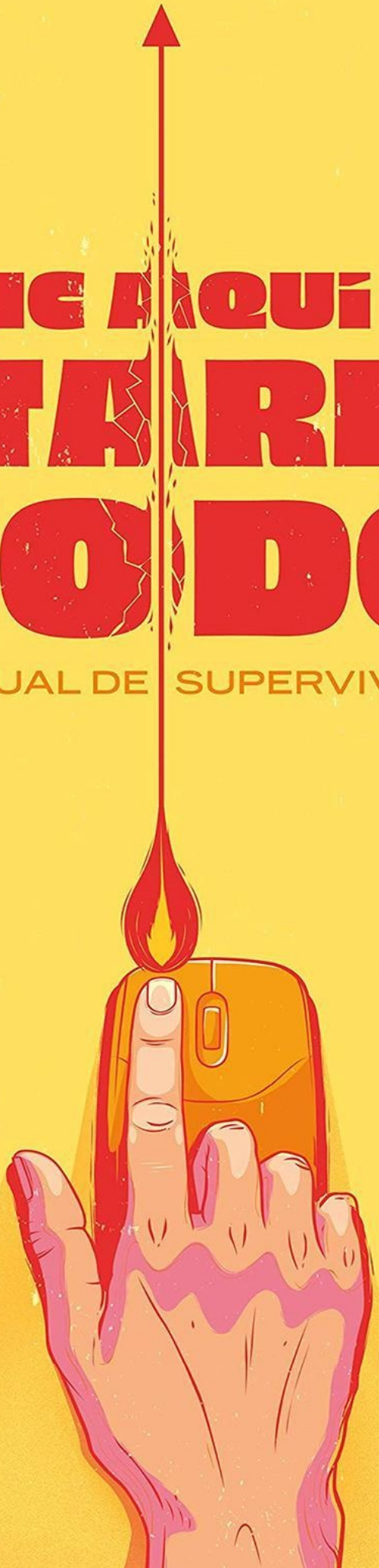
Bruce Schneier

HAZ CLIC AQUÍ PARA MATARLOS A TODOS

UN MANUAL DE SUPERVIVENCIA



¡BLACK MIRROR YA ESTÁ AQUÍ!

Coches autónomos, termostatos y neveras inteligentes, drones equipados con algoritmos de comportamiento… El Internet de las Cosas es una realidad y cuantos más dispositivos estén conectados, más fácil será para alguien muy malo acabar con la vida en este planeta. No es un chiste, tampoco futurología.

Por eso hay que prestar atención a Bruce Schneier, voz autorizada donde las haya en seguridad de internet. Tanto que hasta lo hackers le respetan. Quizá porque mientras todos nos llenamos la boca hablando de robos de datos y cookies, él ya está pensando en cómo pararle los pies al terrorista digital de vanguardia: ese que pronto provocará que los coches se salgan de la carretera, los marcapasos dejen de funcionar, la seguridad de tu casa se desactive o que las impresoras biológicas impriman un virus mortal.

En *Haz clic aquí para matarlos a todos*, Schneier explora los riesgos y las implicaciones de afrontar problemas del siglo XXI con mentalidad del siglo XX y legislación del siglo XIX. No quisiéramos decirte que este libro es urgente, pero todo apunta a que sí.

Bruce Schneier

Haz clic aquí para matarlos a todos

Un manual de supervivencia

ePub r1.0
Titivillus 26.01.2020

Título original: *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*
Bruce Schneier, 2018
Traducción: Álvaro Robledo, 2019

Editor digital: Titivillus
ePub base r2.1

Índice de contenido

Sobre *Haz clic aquí para matarlos a todos*

Schneier guía hábilmente a los lectores a través de ataques que ya han ocurrido, para después enfocarse en aquellos que cree que están a punto de ocurrir. Pero lo más importante es que propone soluciones detalladas que deberían ser lectura obligatoria para políticos de todo el mundo.

Financial Times

Sobrio, lúcido e inteligente, este libro logra diagnosticar cómo surgieron los desafíos en materia de seguridad que plantea la expansión de Internet y propone lo que se debería (aunque probablemente no pase) hacer al respecto.

Nature

Una lectura útil para cualquier persona con conexión a Internet, pero especialmente para aquellas que se preocupan por la privacidad, las libertades civiles y otros temas relacionados.

Kirkus Reviews

Para Arlene, con mis mejores deseos

INTRODUCCIÓN
Todo se está transformando en un ordenador

Considera estos tres incidentes y sus implicaciones.
Escenario 1: En 2015, dos investigadores de seguridad tomaron el control de un Jeep Cherokee. Lo hicieron desde unos dieciséis kilómetros de distancia a través del sistema de entretenimiento del vehículo conectado a Internet. Un vídeo muestra la expresión aterrorizada del impotente conductor circulando por una carretera mientras los piratas informáticos encienden el aire acondicionado, cambian la emisora de radio, accionan los limpiaparabrisas y, al fin, apagan el motor.[1] Dado que esto era una demostración, y no un intento de asesinato, los investigadores no se hicieron con el control de los frenos ni de la dirección, pero podrían haberlo hecho.

No se trata de un truco cualquiera. Los *hackers* han demostrado la existencia de vulnerabilidades en varios modelos de automóviles. Hackearon el puerto de diagnóstico,[2] el reproductor de DVD,[3] el sistema de navegación OnStar[4] y los ordenadores integrados en los neumáticos.[5]

Los aviones también son vulnerables. No se ha hecho una demostración tan vívida como la del Jeep, pero los investigadores de seguridad han afirmado que la aviónica de los aviones comerciales es vulnerable a través del sistema de entretenimiento[6] y de los sistemas de comunicaciones aire-tierra.[7] Durante años los fabricantes de aviones negaron que esto fuera posible, pero al fin, en 2017, el Departamento de Seguridad Nacional de Estados Unidos demostró un pirateo remoto de un Boeing 757,[8] aunque no dio más detalles.

Escenario 2: En 2016, unos piratas informáticos, presumiblemente rusos, detonaron de forma remota un arma cibernética llamada CrashOverride en la subestación eléctrica de alto voltaje de Pivnichna, cerca de Kiev (Ucrania), y la cerraron.[9]

El ataque con la CrashOverride fue diferente del cibernético dirigido contra el centro de control Prykarpattyaoblenergo, en el oeste de Ucrania, el año anterior.[10] Este también causó un apagón, pero fue manual. Allí, los atacantes —también se cree que rusos—[11] obtuvieron acceso al sistema a través de una puerta trasera de *malware* y luego tomaron el control de los ordenadores del centro y apagaron el equipo. (Uno de los operadores de la estación grabó un vídeo de lo que estaba sucediendo)[12]. CrashOverride, por otro lado, lo hizo todo de forma automática.

Al final, las personas a las que la subestación de Pivnichna suministraba su energía tuvieron suerte. Los técnicos desconectaron la planta y restauraron manualmente la energía una hora más tarde. No está claro si las plantas similares de Estados Unidos disponen de los mismos mandos manuales, ni mucho menos del personal con la habilidad para usarlos.

CrashOverride era un arma militar. Se diseñó de forma modular y pudo reconfigurarse con facilidad para una variedad de objetivos: gasoductos, plantas de tratamiento de agua, etc. Tenía otra variedad de *cargas útiles* que ni siquiera se dispararon en el ataque de Ucrania.[13] Podría haber encendido y apagado de manera repetida la subestación, lo que habría dañado físicamente el equipo e interrumpido el suministro de energía durante días o semanas. En medio de un invierno ucraniano habría sido fatal para muchas personas. Y, aunque se disparase esta arma como parte de una operación del Gobierno, también fue una prueba de capacidad.[14] En 2017, hackers desconocidos penetraron en más de veinte centrales eléctricas de Estados Unidos sin causar daños; también fueron pruebas de capacidad.[15]

Escenario 3: Durante un fin de semana en 2017, alguien hackeó 150.000 impresoras en todo el mundo. El pirata informático escribió un programa que detectaba automáticamente las impresoras comunes inseguras y les pedía que imprimieran sin parar mensajes de arte ASCII y de burla.[16] Este tipo de cosas sucede con regularidad y es, sobre todo, vandalismo. A principios de ese mismo año, las impresoras de varias universidades de Estados Unidos fueron hackeadas para imprimir publicidad antisemita.[17]

Aún no hemos visto este tipo de ataque contra las impresoras 3D, pero no hay razón para creer que no sean también vulnerables. Hackear una sola supondría gastos y molestias, aunque esto cambia de forma radical cuando pensamos en las bioimpresoras. Todavía están en los comienzos, pero existe la posibilidad de que los virus personalizados para atacar cánceres u otras enfermedades de pacientes concretos puedan sintetizarse y ensamblarse mediante equipos automatizados.[18]

Imagina un futuro donde esas bioimpresoras sean comunes en hospitales, farmacias y consultorios médicos. Un pirata informático que pueda acceder de manera remota y tenga las instrucciones de impresión adecuadas podría obligar a una bioimpresora a imprimir un virus asesino o una gran cantidad de este, o forzar a muchas a que impriman lotes más pequeños. Dependiendo de cómo se propague el virus, su capacidad infecciosa y su persistencia, podríamos tener una pandemia mundial en nuestras manos.

Haz clic aquí para matarlos a todos, en efecto.

¿Por qué son posibles estos escenarios? Un automóvil de 1998 no era vulnerable a personas que estaban a kilómetros de distancia tratando de hacerse cargo de sus controles. Tampoco lo era una subestación eléctrica en aquel momento. Los modelos actuales son vulnerables y la futura bioimpresora también lo será porque en su núcleo hay ordenadores. Todo se está volviendo vulnerable de esta manera porque todo está convirtiéndose en un ordenador. Más concretamente: un ordenador en Internet.

Tu horno es un ordenador que calienta cosas, tu frigorífico es un ordenador que conserva las cosas frías, tu cámara es un ordenador con una lente y un obturador, un cajero automático es un ordenador con dinero dentro y las bombillas modernas son ordenadores que brillan intensamente cuando alguien, o algún otro ordenador, acciona un interruptor.

Tu coche antes era un artefacto mecánico con algunos ordenadores en él, mientras que ahora es un sistema distribuido entre veinte y cuarenta ordenadores con cuatro ruedas y un motor. Cuando pisas el freno puedes sentir como si estuvieras deteniendo físicamente el vehículo, pero en realidad solo estás enviando una señal electrónica a los frenos; ya no hay una conexión mecánica entre el pedal y las pastillas de freno.

Tu teléfono se convirtió en un poderoso ordenador en 2007, cuando se introdujo el iPhone. Llevamos esos teléfonos inteligentes a todas partes. E *inteligente* es el adjetivo que usamos en los últimos tiempos para estas cosas informatizadas que se encuentran en Internet, lo que significa que pueden recopilar, usar y comunicar datos para operar. Un televisor es inteligente cuando reúne constantemente datos sobre tus hábitos de uso para optimizar tu experiencia.

Pronto los dispositivos inteligentes se incrustarán en nuestros cuerpos. Los marcapasos modernos[19] y las bombas de insulina[20] son inteligentes, las pastillas están volviéndose inteligentes,[21] las lentes de contacto inteligentes no solo mostrarán información basada en lo que ves, sino que también controlarán tus niveles de glucosa y diagnosticarán tu glaucoma,[22] y las

pulseras de actividad son inteligentes y cada vez más capaces de detectar nuestros estados corporales.[23]

Los objetos también están volviéndose inteligentes. Puedes comprar un collar inteligente para tu perro[24] y un juguete inteligente para tu gato.[25] Puedes comprar muchas cosas inteligentes: un bolígrafo,[26] un cepillo de dientes,[27] una taza de café,[28] un juguete sexual,[29] una muñeca Barbie,[30] una cinta métrica[31] o un sensor para tus plantas.[32] Incluso puedes conseguir un casco de motocicleta inteligente que llamará automáticamente a una ambulancia y le enviará un mensaje de texto a tu familia si tienes un accidente.[33]

Ya estamos viendo los inicios de las casas inteligentes. La asistente virtual Alexa y sus primos escuchan tus órdenes y responden. Hay termostatos inteligentes,[34] enchufes inteligentes[35] y aplicaciones inteligentes. Puedes comprar una báscula de baño inteligente[36] y un inodoro inteligente.[37] Puedes comprar bombillas inteligentes y un centro inteligente para controlarlas.[38] También puedes comprar una cerradura de puerta inteligente, que te permitirá darles a los técnicos de reparación y al personal de entrega un código único para entrar en tu hogar,[39] y una cama inteligente que detectará tus patrones de sueño y diagnosticará tus trastornos asociados.[40]

En los lugares de trabajo, muchos de esos mismos dispositivos inteligentes están conectados en red con cámaras de vigilancia, sensores que detectan los movimientos de los clientes y todo lo demás. Los sistemas inteligentes en edificios se encargarán de que la iluminación sea eficiente, del mecanismo de los ascensores, del control del clima y de otros servicios.

Las ciudades están empezando a integrar sensores inteligentes en las carreteras, el alumbrado público y en las aceras de las plazas, así como redes eléctricas inteligentes y redes de transporte inteligentes.[41] Pronto las ciudades podrán controlar tus electrodomésticos y otros aparatos del hogar para optimizar el uso de la energía. Las redes de vehículos inteligentes sin conductor se dirigirán automáticamente hacia donde se necesiten minimizando así el uso de energía en el proceso. Los sensores y controles en las calles regularán mejor el tráfico, acelerarán los tiempos de respuesta de la policía y de los paramédicos e informarán sobre inundaciones en las carreteras. Otros sensores mejorarán la eficiencia de los servicios públicos, desde el envío de policías hasta la optimización de las rutas de los camiones de basura y la reparación de baches. Las vallas publicitarias inteligentes te reconocerán cuando pases y te mostrarán publicidad adaptada para ti.[42]

Una subestación eléctrica es, en realidad, solo un ordenador que distribuye electricidad y, como todo lo demás, está en Internet. CrashOverride no infectó la subestación de Pivnichna directamente, sino que estaba escondido en los ordenadores de una sala de control a miles de kilómetros conectada a la estación a través de Internet.

Este cambio tecnológico ocurrió durante la última década más o menos. Antes las cosas tenían ordenadores en ellas; ahora *son* ordenadores con cosas unidas a ellos. Y, a medida que los ordenadores continúan haciéndose más pequeños y más baratos, están incorporándose a más cosas y otras están convirtiéndose ellas mismas en ordenadores. Es posible que no lo notes y, por supuesto, no compras automóviles y frigoríficos como si fueran ordenadores, sino por sus funciones de transporte y refrigeración. Pero son ordenadores, y eso es importante cuando hablamos de seguridad.

Nuestra concepción de Internet también está cambiando. Ya no vamos a un lugar específico en nuestros hogares u oficinas e iniciamos sesión en lo que parece ser un espacio separado. Ya no entramos en una sala de chat, descargamos nuestro correo electrónico o, en muchos casos, navegamos por Internet. Esas metáforas espaciales ya no tienen sentido, y en unos años decir «voy a meterme en Internet» tendrá tanto sentido como conectar una tostadora y decir «me voy a la red eléctrica».[43]

El nombre que se le da a esta conectividad ubicua es *Internet de las cosas* (IoT, por sus siglas en inglés). Es sobre todo un término de marketing, pero también es muy real. La firma de análisis de tecnología Gartner la define como «la red de objetos físicos que contienen tecnología incorporada para comunicarse y detectar o interactuar con sus estados internos o el entorno externo».[44] Se trata de conectar todo tipo de dispositivos a través de Internet y dejar que hablen —a nosotros, entre ellos y con diferentes aplicaciones informáticas.

La magnitud de este cambio es asombrosa. En 2017, había 8.400 millones de cosas conectadas a Internet, principalmente ordenadores y teléfonos, un aumento de un tercio respecto al año anterior.[45] Para 2020, es probable que haya entre 20.000 y 75.000 millones, dependiendo de qué estimaciones creas.[46]

Este crecimiento explosivo proviene de proveedores que buscan una ventaja competitiva o que quieren estar al día con la competencia y deciden que el truco está en que sus productos sean *inteligentes*. Cuanto más pequeños se vuelvan los ordenadores, e incluso más baratos, comenzaremos a verlos en más lugares.

Tu lavadora ya es un ordenador que limpia la ropa. Cuando los ordenadores más nuevos, más baratos y mejor integrados tengan conectividad a Internet, será más fácil para el fabricante de tu lavadora incluir esa función, por lo que luego será más complicado para ti comprar una nueva sin ella.

Hace dos años intenté, sin éxito, comprar un coche nuevo sin conexión a Internet. Había algunos vehículos en venta sin conectividad, pero era algo estándar en todos los que yo quería. A medida que el precio de estas tecnologías disminuya, esto sucederá con todo. Internet se convertirá en parte de los dispositivos más baratos y menos versátiles hasta que sea una característica estándar.

Ahora mismo, puede parecer algo tonto que tu lavadora tenga conexión a Internet e imposible que tu camiseta algún día la tenga,[47] pero en pocos años será lo usual. Los ordenadores son cada vez más poderosos, más pequeños y más baratos; la ropa conectada será lo habitual cuando el beneficio que obtenga el minorista con la automatización de los procesos de preventa con seguimiento de inventario y de uso posventa sea mayor que el coste de un microprocesador. En las próximas décadas es posible que no puedas comprar una camiseta sin sensor, y para entonces darás por sentado que tu lavadora hable con la ropa que está lavando y determine el ciclo y el detergente óptimos, y luego venda la información sobre lo que te pones (y lo que no) a los fabricantes de ropa.

Siempre que hablo de este tema hay personas que preguntan por qué. Pueden entender que se ahorre energía, pero no por qué alguien pondría su cafetera o cepillo de dientes en Internet. «El “Todo Inteligente” se ha vuelto oficialmente estúpido», reza un titular de 2016 sobre un primer intento de frigorífico conectado a Internet.[48]

La respuesta es simple: la economía de mercado. Si el coste de los dispositivos informatizados disminuye, el beneficio marginal también lo hace, ya sea en las características proporcionadas o en los datos de vigilancia recopilados necesarios para justificar la informatización. Esto podría ser beneficioso para el usuario en términos de características adicionales, o para el fabricante en términos de información y marketing para su base de datos de usuarios. Al mismo tiempo, los proveedores de chips se están alejando de la especialización en favor de la fabricación de chips de propósito general, más baratos y de producción masiva. Conforme estos ordenadores integrados se estandaricen, será menos caro para los fabricantes incluir la conectividad que eliminarla. Literalmente, será más barato ensuciar la ciudad con sensores que limpiar la basura de las aceras.

Dotar de *inteligencia* y conectividad a todo tiene ventajas; algunas podemos verlas hoy y otras solo las advertiremos una vez que estos ordenadores hayan alcanzado una masa crítica. El Internet de las cosas se integrará en todos los niveles de nuestras vidas, y no creo que podamos predecir las características nacientes de esta tendencia. Estamos llegando a un cambio fundamental debido a la escala y al alcance; estas diferencias en grado están causando una diferencia en especie. Todo está convirtiéndose en un sistema complejo e hiperconectado en el que, incluso aunque las cosas no interactúen entre sí, están en la misma red y se influyen unas a otras.

Aparte del Internet de las cosas, esta tendencia va más allá. Partamos del IoT, o, más general, de los sistemas ciberfísicos. Añade la miniaturización de sensores, controladores y transmisores. Suma a esto algoritmos autónomos, aprendizaje automático e inteligencia artificial. Aprovecha la computación en la nube con los aumentos correspondientes en las capacidades de almacenamiento y procesamiento. No olvides incluir la penetración de Internet, la computación ubicua y la disponibilidad de conectividad inalámbrica de alta velocidad. Y, por último, combínalo todo con un poco de robótica. Lo que obtienes es un único Internet global que afecta al mundo de una manera física directa. Es un Internet que siente, piensa y actúa.[49]

Estas no son tendencias distintas, sino que convergen, se construyen y se refuerzan entre ellas. La robótica utiliza algoritmos autónomos. Los drones combinan el Internet de las cosas, la autonomía y la computación móvil; y las vallas publicitarias inteligentes, la personalización con el Internet de las cosas. Un sistema que regula automáticamente el agua que fluye sobre una presa combina sistemas ciberfísicos, agentes autónomos y es probable que computación en la nube.

Y, aunque nos guste pensar de otra manera, los humanos somos solo otro componente entre muchos de estos sistemas. Proveemos de insumos a los ordenadores y aceptamos sus resultados —somos los consumidores de su funcionalidad automatizada—, proporcionamos interconexiones y comunicaciones a aquellos sistemas que no se han vuelto lo bastante inteligentes como para salir del ciclo, movemos a los que no son físicamente autónomos y les influimos igual que ellos nos influyen a nosotros. En un grado muy real, nos convertiremos en cíborgs virtuales, incluso aunque estos dispositivos sigan siendo independientes de nuestra fisiología.

Necesitamos un nombre para este nuevo sistema de sistemas. Es más que Internet, más que el Internet de las cosas. En realidad, es Internet + Cosas. Más preciso: Internet + Cosas + Nosotros. O, para abreviar, Internet+.[50] Para

ser sincero, me gustaría no tener que acuñar un término, pero no puedo encontrar uno existente que describa la apoteosis de todas esas tendencias. Por lo tanto, al menos para este libro, será Internet+.

Por supuesto, palabras como *inteligente* y *pensar* son relativas. En este punto, son más aspiracionales que otra cosa. Gran parte del Internet de las cosas no es muy inteligente, y gran parte será estúpido durante mucho tiempo, pero continuará haciéndose más inteligente. Y, si bien es muy poco probable que veamos ordenadores conscientes en un futuro cercano, los ordenadores ya se comportan de manera inteligente en tareas específicas. El Internet+ se está volviendo más poderoso gracias a todas las interconexiones que estamos construyendo. También se está volviendo menos seguro. Este libro cuenta la historia de por qué esto es así y qué podemos hacer al respecto.

Es una historia complicada y la cuento en dos partes. En la primera, describo el estado actual de la seguridad informática, técnica, política y económica, así como las tendencias que nos han traído hasta aquí. Los ordenadores se están volviendo más pequeños y más partidarios de manipular el mundo físico, pero siguen siendo básicamente los mismos ordenadores con los que hemos estado trabajando durante décadas. Los problemas técnicos de seguridad siguen sin cambios, las cuestiones sobre política son las mismas contra las que hemos estado luchando y, a medida que los ordenadores y las comunicaciones se integran en todo, las diferentes industrias comenzarán a parecerse a la de los ordenadores. La seguridad informática hará que sea todo sobre seguridad, y las lecciones de seguridad informática se aplicarán en todas partes. Y si sabemos algo acerca de los ordenadores —ya sean vehículos, subestaciones eléctricas o impresoras biológicas—, es que son vulnerables a los ataques de aficionados, activistas, delincuentes, Estados nación y cualquiera con capacidades técnicas.

En el capítulo 1 hago un somero repaso de todas las razones técnicas por las que Internet es tan inseguro. En el capítulo 2 analizo la manera en que, principalmente, mantenemos la seguridad en nuestros sistemas —parcheando las vulnerabilidades cuando se descubren— y por qué fallará en Internet+. El capítulo 3 trata sobre cómo probamos quiénes somos en Internet y cómo podemos ocultarlo. En el capítulo 4 explico las fuerzas políticas y económicas que favorecen la inseguridad: el capitalismo de vigilancia, la ciberdelincuencia, la guerra cibernética y las prácticas corporativas y gubernamentales más invasivas que se nutren de la inseguridad.

Por último, en el capítulo 5 describo por qué los riesgos aumentan y cómo se volverán catastróficos. *Haz clic aquí para matarlos a todos* es una

hipérbole, pero ya estamos viviendo en un mundo donde los ataques informáticos pueden bloquear vehículos y deshabilitar las centrales eléctricas, acciones ambas que pueden dar como resultado muertes catastróficas si se realizan a gran escala. Añade a esto ataques contra aviones o dispositivos médicos y contra casi toda nuestra infraestructura crítica global, y tendremos que considerar algunos escenarios bastante aterradores.

Si eres lector habitual de mis libros, artículos y blog, esta primera parte te servirá como repaso. Si eres nuevo en todo esto, estos capítulos son una base importante para lo que está por venir.

Lo que sucede con la seguridad de Internet+ es que todos estamos acostumbrados a ella. Hasta ahora y por lo general, le hemos dejado al sector la seguridad informática y de Internet, un enfoque que ha funcionado bastante satisfactoriamente, más que nada porque no tenía demasiada importancia, ya que la seguridad tenía que ver bastante con la privacidad y mucho con los bits. Si hackeaban tu ordenador, perdías algunos datos importantes o te robaban la identidad; podía ser algo odioso e incluso costoso, pero no era catastrófico. Ahora que todo es un ordenador, las amenazas se dirigen contra la vida y la propiedad. Los piratas informáticos pueden estrellar tu coche, desactivar tu marcapasos o acabar con la red eléctrica de la ciudad: eso es una catástrofe.

En la segunda parte de este libro discuto los cambios necesarios en las políticas que protegen Internet+. Los capítulos 6, 7 y 8 tratan sobre qué, cómo y quién debe mejorar la seguridad de Internet+. Nada de esto es nuevo o complicado; el problema está en los detalles. Cuando llegues al capítulo 8, espero convencerte de que el quién es el Gobierno. Si bien existe un riesgo considerable en otorgarle al Gobierno este rol, no hay una alternativa viable. El actual estado de dejadez de la seguridad de Internet+ es el resultado de incentivos empresariales mal alineados, de un Gobierno que prioriza los usos ofensivos de Internet sobre la defensa, de los problemas de acción colectiva y los fallos del mercado que deben repararse y que requieren una intervención. Una de las cosas que propongo en el capítulo 8 es un nuevo organismo gubernamental que coordine y asesore a otros organismos sobre las políticas y la tecnología de seguridad de Internet+. Puedes estar en desacuerdo conmigo, está bien, aunque es un debate que debemos tener.

El capítulo 9 es más general. Para ser fiable, el Gobierno debe priorizar la defensa, y no la ofensa. Describo cómo llevarlo a cabo.

Hablando en términos prácticos, es poco probable que muchos de los cambios en las políticas que propongo en los capítulos 6 al 9 se realicen a

corto plazo. Por tanto, en el capítulo 10 intento ser más realista y analizo qué es probable que suceda y qué podemos hacer para responder, tanto en Estados Unidos como en otros países. El capítulo 11 trata sobre algunas propuestas en las políticas actuales que, en efecto, dañarán la seguridad de Internet+. El capítulo 12 también es general y analiza cómo podemos crear un Internet+ en donde la confianza, la capacidad de recuperación y la paz sean la norma, y cómo podría ser.

Fundamentalmente, estoy argumentando a favor de un buen Gobierno que haga el bien. Puede ser una postura difícil de defender, sobre todo en la industria de los ordenadores —antirregulación, fuertemente libertaria y de pequeño gobierno—, pero es importante.[51] Todos hemos escuchado hablar sobre las formas en que el Gobierno comete errores, hace mal su trabajo o interfiere con el progreso tecnológico. Menos discutido es cómo el Gobierno dirige los mercados, protege a los individuos y actúa como un contrapeso del poder corporativo. Una de las principales razones por las que Internet+ es tan inseguro hoy en día es la ausencia de supervisión gubernamental. Cuanto más catastróficos se vuelven los riesgos, más necesitamos que el Gobierno se involucre.

Termino este libro con una llamada a la acción para los políticos y los tecnólogos. Estas discusiones políticas son inherentemente técnicas. Necesitamos políticos que entiendan de tecnología y que los tecnólogos participen en política. Necesitamos que el campo de los tecnólogos sea de interés público. Esta necesidad se presenta en más ámbitos que en el de la seguridad en Internet+, pero me centro en el tecnológico porque es el que conozco.

Varios temas adicionales se tejen a lo largo del libro:

- La carrera de armamentos para la seguridad. A menudo es útil considerar la seguridad como una carrera tecnológica de armamentos entre el atacante y el defensor. El atacante desarrolla una nueva tecnología, y el defensor desarrolla una contratecnología como respuesta o una nueva tecnología defensiva que obliga a los atacantes a adaptarse de alguna otra manera. La forma en la que se desarrolla esta carrera de armamentos en Internet+ es fundamental para comprender la seguridad de Internet.
- Confianza. Aunque no solemos pensar en ello, la confianza es fundamental para el funcionamiento de la sociedad en todos los niveles. En Internet la confianza está en todas partes. Confiamos en los

ordenadores, en el *software* y en los servicios de Internet que usamos. Confiamos en las partes de la Red que no podemos ver y en el proceso de fabricación de los dispositivos que utilizamos. La forma en la que mantenemos esta confianza y cómo se socava también son fundamentales para comprender la seguridad en Internet+.

- Complejidad. Todo sobre este problema es complejo: la tecnología, las normas, la interacción entre la tecnología y esas normas; también la política, la economía y la sociología. Es complejo en muchas dimensiones y su complejidad aumenta con el tiempo. La seguridad de Internet+ es lo que conocemos como un *problema serio*, lo que no significa que sea malo, sino que es difícil o imposible de resolver porque es complicado incluso definir el problema y las necesidades, y mucho más encontrar una solución adecuada.

Este libro abarca mucho terreno, lo que quiere decir que se trata gran parte de forma rápida y somera. Las extensas notas finales están destinadas a ser tanto referencias como invitaciones a lecturas adicionales, y todas se verificaron a finales de abril de 2018. También están en el sitio web del libro, donde se encuentran enlaces: https://www.schneier.com/ch2ke.html. Si hay actualizaciones del libro, las encontrarás ahí. En Schneier.com tienes mi boletín mensual de correo electrónico y mi blog actualizado a diario sobre estos temas, así como todos mis otros escritos.

Veo estos problemas desde otro nivel. Soy tecnólogo de corazón, no legislador ni analista político. Puedo describir las soluciones tecnológicas a nuestros problemas de seguridad e incluso explicar el tipo de políticas necesarias para identificar, generar e implementar esas soluciones tecnológicas, pero no escribo sobre política ni sobre planes de acción. No puedo decirte cómo obtener apoyo para los cambios en las políticas, ni si es factible. Esto supone un agujero enorme en el libro y lo acepto.

También hay que tener en cuenta que escribo desde una perspectiva estadounidense, así que casi todos los ejemplos son de Estados Unidos y la mayoría de las recomendaciones se refieren a este país. Por un lado, es lo que mejor conozco, aunque también creo que Estados Unidos sirve como un ejemplo excepcional de cómo las cosas salieron mal y, debido a su tamaño y posición en el mercado, se encuentra en un lugar singular para cambiar las cosas y mejorarlas. Si bien este no es un libro sobre temas internacionales ni sobre geopolítica de la seguridad de Internet,[52] algunos de estos aspectos aparecen en distintos capítulos.

Estos asuntos están en constante evolución, y un libro como este es necesariamente una instantánea en el tiempo. Recuerdo cuando terminé *Data y Goliat* en marzo de 2014; pensé en que se publicaría seis meses después y esperé que no pasara nada que cambiara la narrativa del libro mientras tanto. Ahora siento lo mismo, y también confío en que no suceda nada tan importante que requiera una reescritura. Es verdad que surgirán nuevas historias y ejemplos, aunque es probable que el paisaje que describo aquí perdure durante muchos años.

El futuro de la seguridad de Internet+ —o de la ciberseguridad, si tienes una inclinación militar— es un tema muy amplio, y la mayoría de los capítulos de este libro podrían ser, cada uno de ellos, libros en sí mismos. Al ofrecer amplitud en lugar de profundidad, espero que los lectores tengan una visión general de la situación, que se entiendan los problemas y que podamos elaborar una hoja de ruta hacia una posible mejora. Mis objetivos son atraer a un público más numeroso a este importante debate y ayudar a educar a las personas para una discusión más informada. Tomaremos decisiones importantes en los próximos años, incluso aunque lo único que hagamos sea elegir no hacer nada.

Estos riesgos no van a desaparecer. No están al margen de países con infraestructuras menos desarrolladas o Gobiernos más totalitarios, no disminuyen aunque descubramos el desorden de nuestro disfuncional sistema político en Estados Unidos y no van a resolverse mágicamente por las fuerzas del mercado. Los habremos resuelto cuando nos decidamos a ello de forma consciente y aceptemos los costes políticos, económicos y sociales de nuestras soluciones.

El mundo está hecho de ordenadores y necesitamos protegerlos. Para ello tenemos que pensar de manera diferente. En una conferencia de seguridad de Internet de 2017, Tom Wheeler, expresidente de la FCC, parafraseó a la exsecretaria de Estado Madeleine Albright diciendo lo siguiente: «Nos estamos enfrentando a problemas del siglo I, discutiéndolos en términos del siglo y proponiendo soluciones del siglo XIX».[53] Está en lo cierto y tenemos que hacerlo mejor. Nuestro futuro depende de ello.

Minneapolis, Minnesota y Cambridge (Massachusetts),
abril de 2018

PRIMERA PARTE
LAS TENDENCIAS

HACE UN PAR DE AÑOS reemplacé mi termostato. Viajo mucho y quería ahorrar energía los días que no estaba en casa. Mi nuevo termostato es un ordenador conectado a Internet que controlo desde mi teléfono inteligente: puedo configurar programas para cuando estoy en casa y para cuando estoy fuera y controlar la temperatura dentro, todo de forma remota; es perfecto.

Por desgracia, también le abrí la puerta a algunos problemas potenciales. En 2017, un hacker se jactó en Internet de haber secuestrado de forma remota el termostato inteligente Heatmiser (no era de la misma marca que el mío).[1] Por otro lado, un grupo de investigadores demostró que había *ransomware*[2] en dos marcas populares de termostatos estadounidenses (tampoco la del mío) y exigían pagos en bitcoins para renunciar a su control.[3] Si pudieron infectarlo con ransomware, también podrían haber secuestrado el termostato en una red robot y utilizarlo para atacar otros sitios en Internet. Este fue un proyecto de investigación, ningún termostato operacional resultó dañado en el proceso, ni se rompieron las tuberías de agua; pero la próxima vez podría ser mi marca y no ser tan inofensivo.[4]

Internet+ significa dos cosas cuando hablamos de seguridad.

Una, las propiedades de seguridad de nuestros ordenadores y teléfonos inteligentes se convertirán en las propiedades de seguridad de todo. Por tanto, cuando pienses en la inseguridad del software o en los problemas de inicio de sesión y autenticación, o en las vulnerabilidades de seguridad y las actualizaciones del software (todos los temas que trataremos en la primera parte de este libro), ya no solo tendrá que ver con los ordenadores y los teléfonos, sino con termostatos, automóviles, frigoríficos, audífonos implantados, cafeteras, farolas, señales de tráfico y todo lo demás. La seguridad informática se convertirá en la seguridad de todas las cosas.

Y dos, las lecciones de seguridad informática serán aplicables a todo. Quienes hemos estado en el campo de la seguridad informática hemos aprendido mucho en las últimas décadas: acerca de la carrera de armamentos entre atacantes y defensores, de la naturaleza de los fallos informáticos y de la necesidad de resiliencia; una vez más, todos los temas a los que nos

enfrentamos. Hablaré más adelante de todo ello. Estas lecciones antes solo trataban sobre los ordenadores; ahora lo engloban todo.

Existe una diferencia crítica: los riesgos son mucho mayores.

Los riesgos de un Internet que afecta al mundo de una manera física directa son cada vez más catastróficos. Las amenazas de hoy incluyen la posibilidad de que los piratas informáticos estrellen aviones a distancia,[5] bloqueen vehículos[6] y jueguen con dispositivos médicos para asesinar a personas.[7] Nos preocupa que nos pirateen con aparatos GPS que desvíen los envíos globales de correo[8] y que manipulen los recuentos de votos electrónicos para cambiar las elecciones. Con casas inteligentes, los ataques pueden significar daños a la propiedad;[9] con los bancos, el caos económico; con las centrales eléctricas, apagones; con las plantas de tratamiento de residuos, derrames tóxicos; con automóviles, aviones y dispositivos médicos, pueden significar la muerte, y con los terroristas y los Estados nación, la seguridad de economías enteras y países podría estar en juego.

La seguridad es una carrera de armamentos entre el atacante y el defensor. Piensa en la batalla entre los anunciantes de Internet y los bloqueadores de anuncios. Si usas un bloqueador —aproximadamente seiscientos millones de personas en el mundo lo hacen—,[10] notarás que algunos sitios ahora bloquean a los bloqueadores de anuncios para evitar que veas los contenidos hasta que los deshabilites.[11] El *spam* es una lucha entre los *spammers*, que desarrollan nuevas técnicas, y las compañías antispam averiguando cómo combatirlos.[12] El fraude de clics es muy parecido: los estafadores usan varios trucos para convencer a compañías como Google de que les deben dinero porque personas reales han hecho clic en los enlaces web mientras Google intenta detectarlos. El fraude con tarjetas de crédito es otra guerra continua entre los atacantes, que desarrollan técnicas distintas, y las compañías de tarjetas de crédito, que los combaten con nuevas formas de prevención y detección. Los cajeros automáticos modernos son el resultado de un enfrentamiento de décadas entre atacantes y defensores, uno que continúa hoy en día con *skimmers*[13] cada vez más pequeños y más discretos para robar información de tarjetas y los números PIN,[14] e incluso llevar a cabo ataques remotos contra cajeros automáticos a través de Internet.[15]

Así que, para entender la seguridad de Internet+, debemos comenzar por comprender el estado actual de la seguridad de Internet. Debemos entender las tendencias tecnológicas, comerciales, políticas y delictivas que nos han llevado a esta situación y que continúan en vigor, así como las tendencias

tecnológicas que definen y limitan lo que es posible e ilustran lo que se avecina.

01

LOS ORDENADORES TODAVÍA SON DIFÍCILES DE PROTEGER

LA SEGURIDAD ES SIEMPRE UNA CONTRAPARTIDA. A menudo es la seguridad frente a la comodidad, pero a veces es la seguridad contra las características o el rendimiento. Que prefiramos todas esas cosas por encima de la seguridad es la mayor razón por la que los ordenadores no son seguros, pero también es cierto que protegerlos es muy difícil.

En 1989, el famoso experto en seguridad de Internet Gene Spafford dijo que «el único sistema verdaderamente seguro es el que se apaga, se coloca en un bloque de hormigón y se sella en una habitación revestida de plomo con guardias armados, y aún así tengo mis dudas».[1] Casi treinta años después sigue siendo así.

Es cierto para los ordenadores independientes y para los ordenadores integrados conectados a Internet y que están en todas partes. Hace poco, Rod Beckstrom, exdirector del Centro Nacional de Seguridad Cibernética, lo resumió de esta manera: 1) cualquier cosa conectada a Internet puede ser pirateada; 2) todo se está conectando a Internet; 3) como resultado, todo se vuelve vulnerable.[2]

Sí, los ordenadores son tan difíciles de proteger que cada investigador de seguridad tiene su propio dicho al respecto. Aquí está el mío del año 2000: «La seguridad es un proceso, no un producto».[3]

Hay muchas razones por las que esto es así.

LA MAYORÍA DEL SOFTWARE ESTÁ MAL ESCRITO Y ES INSEGURO

Juego a Pokémon Go en mi teléfono y el juego se bloquea todo el tiempo;[4] su inestabilidad es extrema, pero no excepcional. Todos lo hemos experimentado: nuestros ordenadores y teléfonos móviles fallan con

frecuencia, los sitios web no se cargan o las funciones no van. Hemos aprendido a compensar esta situación: guardamos de forma compulsiva nuestros datos y hacemos copias de seguridad de nuestros archivos o utilizamos sistemas que lo hacen por nosotros de forma automática, reiniciamos nuestros ordenadores cuando empiezan a comportarse de manera extraña y algunas veces perdemos datos importantes;[5] sin embargo, no esperamos que nuestros ordenadores funcionen tan bien como los productos de consumo típicos de nuestras vidas, a pesar de que nos frustramos continuamente cuando no lo hacen.

El software está mal escrito porque, salvo algunas excepciones, el mercado no premia que sean de buena calidad. «Bueno, rápido, barato: elige dos». Para el mercado, que sea barato y rápido es más importante que la calidad. Para la mayor parte de nosotros, los softwares mal escritos han sido lo bastante buenos casi siempre.

Esta filosofía ha permeado la industria a todos los niveles. Las empresas no recompensan la calidad del software de la misma manera que premian la entrega de productos antes de lo programado y por debajo del presupuesto. Las universidades se centran más en el código que apenas funciona que en el que es fiable. Y la mayoría de los consumidores no están dispuestos a pagar lo que costaría hacerlo mejor.

El software moderno está plagado de errores, algunos de ellos inherentes a su propia complejidad (hablaremos sobre ello más adelante), pero casi todos son errores de programación[6] que no fueron corregidos durante el proceso de desarrollo y permanecen en el software después de que se haya terminado y enviado. Que este tipo de software funcione deja patente lo bien que podemos diseñar softwares llenos de errores.

Por supuesto, no todos los procesos de desarrollo de software son iguales. Microsoft pasó la década posterior a 2002 mejorando su proceso de desarrollo de software para minimizar la cantidad de vulnerabilidades de seguridad en el software enviado.[7] Sus productos no son, de ninguna manera, perfectos, eso está más allá de las capacidades de las tecnologías de hoy en día, pero son mucho mejores que la media. Por otro lado, Apple es conocida por su software de calidad,[8] al igual que Google; algunas piezas de software muy pequeñas y críticas son de alta calidad; el software de aviónica para aeronaves está escrito con un estándar mucho más riguroso que el resto, y la NASA utilizó un famoso proceso de control de calidad para el software de su transbordador espacial.[9]

Las razones por las cuales estas son excepciones varían entre industrias y de una compañía a otra: las empresas de sistemas operativos gastan mucho dinero, es fácil obtener pequeñas rutinas de código y el software de los aviones está muy regulado. La NASA todavía tiene estándares de garantía de calidad demasiado conservadores.[10] Incluso con los sistemas de software de alta calidad, como Windows, macOS, iOS y Android, siempre estás instalando parches.

Algunos errores y virus son también vulnerabilidades en la seguridad, y algunas de ellas pueden explotarlas los atacantes. Un ejemplo que ilustra esto es el desbordamiento de búfer:[11] un error de programación que le permite a un atacante, en algunos casos, forzar el programa para que ejecute comandos arbitrarios y tomar el control del ordenador. Existen muchas áreas con errores potenciales como este, aunque algunos son más fáciles de cometer que otros.

Aquí los números son difíciles de precisar. No sabemos qué porcentaje de errores también son vulnerabilidades ni qué porcentaje de vulnerabilidades pueden aprovecharse, y existe un debate académico legítimo sobre si estos errores aprovechables son escasos o abundantes.[12] Me decanto por lo más abundante: los grandes sistemas de software tienen miles de vulnerabilidades aprovechables y penetrar en ellos es cuestión de encontrarlas —a veces resulta simple, otras no.

Pero, aunque las vulnerabilidades sean abundantes, no se distribuyen uniformemente; hay algunas más fáciles de encontrar y otras más difíciles. La seguridad del software mejora en gran medida gracias a las herramientas que encuentran y corrigen de manera automática categorías enteras de vulnerabilidades, y a las prácticas de codificación que eliminan muchas de las que se encuentran con facilidad. Cuando una persona encuentra una vulnerabilidad, es probable que alguien más lo haga o que pronto vaya a hacerlo. Heartbleed es una vulnerabilidad en la seguridad web que permaneció dos años sin ser descubierta, y luego dos investigadores independientes la encontraron con pocos días de diferencia.[13] Las vulnerabilidades de Spectre y Meltdown en los chips de los ordenadores existieron durante al menos diez años antes de que varios investigadores las descubrieran en 2017.[14] No he visto ninguna otra explicación para este descubrimiento paralelo aparte de que ocurre; pero será algo importante cuando hablemos de los Gobiernos que almacenan vulnerabilidades para espionaje y ciberarmas en el capítulo 9.

El auge de los dispositivos IoT (Internet de las cosas) supone más software, más líneas de código e incluso más errores y vulnerabilidades. Los

dispositivos IoT baratos significan programadores menos capacitados, procesos de desarrollo de software más descuidados y más reutilización de códigos,[15] y, por lo tanto, un mayor impacto de una vulnerabilidad única si se difunde ampliamente.

El software del que dependemos —que se ejecuta en nuestros ordenadores y teléfonos, en nuestros automóviles y dispositivos médicos, en Internet, en los sistemas que controlan nuestra infraestructura crítica— es inseguro de múltiples maneras. Esto no es solo cuestión de encontrar las escasas vulnerabilidades y corregirlas, ya que existen demasiadas como para hacerlo, sino un hecho de la vida del software con el que tendremos que convivir en el futuro inmediato.

INTERNET NO FUE DISEÑADO TENIENDO EN CUENTA LA SEGURIDAD

En abril de 2010, durante unos dieciocho minutos, el 15 % de todo el tráfico de Internet pasó de pronto a través de servidores en China de camino hacia su destino.[16] No sabemos si fue el Gobierno chino probando su capacidad de interceptación o un error real, pero sabemos cómo lo hicieron los atacantes: abusaron del protocolo de frontera.

El protocolo de frontera o de puerta de enlace (BGP, por sus siglas en inglés) es la forma en la que Internet dirige físicamente el tráfico por varios cables y otras conexiones entre proveedores de servicios, países y continentes. Debido a que no hay autenticación en el sistema y todos confían de manera implícita en la información sobre la velocidad y la congestión, el BGP puede manipularse.[17] Sabemos, gracias a los documentos divulgados por el contratista del Gobierno Edward Snowden, que la Agencia de Seguridad Nacional de Estados Unidos (NSA, por sus siglas en inglés) usa esta inseguridad inherente para hacer que ciertos flujos de datos sean más fáciles de observar.[18] En 2013, una empresa informó sobre 38 casos diferentes en los que el tráfico de Internet se desvió a rúters de proveedores de servicios bielorrusos o islandeses.[19] En 2014, el Gobierno turco utilizó esta técnica para censurar partes de Internet.[20] En 2017, el tráfico hacia y desde varios de los principales PSI (prestadores de servicios de Internet) de Estados Unidos se redirigió durante un breve espacio de tiempo a un proveedor de Internet ruso desconocido.[21] Y no creas que este tipo de ataques se limita a los Estados nación; una charla de 2008 en la conferencia de piratas informáticos de DefCon mostró cómo cualquiera puede hacerlo.[22]

Cuando se desarrolló Internet, la seguridad se centraba en los ataques físicos contra la Red. Su arquitectura tolerante con los errores puede encargarse de servidores y conexiones que fallan o rotas. Lo que no puede hacer es afrontar ataques sistémicos contra los protocolos subyacentes.

Los protocolos básicos de Internet se desarrollaron sin tener en mente la seguridad, y muchos de ellos siguen siendo inseguros a día de hoy. No hay seguridad en la línea del remitente de un correo electrónico: cualquiera puede fingir ser otra persona. No hay seguridad en el sistema de nombres de dominio (DNS, por sus siglas en inglés), que traduce las direcciones de Internet de nombres legibles por personas a direcciones numéricas legibles por ordenadores, o en el protocolo de tiempo de red, que mantiene todo sincronizado. No hay seguridad en los protocolos HTML originales que conforman la World Wide Web, y el protocolo HTTPS, más seguro todavía, tiene muchas vulnerabilidades. Los atacantes pueden sabotear todos estos protocolos.

Estos protocolos se inventaron en los años setenta y principios de los ochenta, cuando Internet se limitaba a instituciones de investigación y no se utilizaba para nada crítico. David Clark, profesor del MIT y uno de los arquitectos del antiguo Internet, recuerda: «No es que no hayamos pensado en la seguridad. Sabíamos que había personas poco fiables por ahí, y pensamos que podríamos excluirlas».[23] Sí, de verdad pensaron que podían limitar el uso de Internet a personas conocidas.

En 1996, la idea predominante era que la seguridad sería responsabilidad de la última etapa; es decir, de los ordenadores situados enfrente de las personas, y no de la Red. Aquí encontramos la opinión al respecto del Grupo de Trabajo de Ingeniería de Internet (IETF), el organismo que establece los estándares de la industria para Internet, en 1996:

> Es altamente deseable que los operadores de Internet protejan la privacidad y la autenticidad de todo el tráfico, pero esto no es un requisito de la arquitectura. La confidencialidad y la autenticación son responsabilidad de los usuarios finales y deben implementarse en los protocolos utilizados por dichos usuarios. Los puntos finales no deben confiar en la confidencialidad o la integridad de los operadores. Los operadores pueden optar por proporcionar cierto nivel de protección, pero esto es algo secundario a la responsabilidad principal de los usuarios finales de protegerse a sí mismos.[24]

Obviamente, esto no es ninguna tontería. En el capítulo 6 hablaremos sobre el modelo de red de extremo a extremo (*end-to-end*), lo que significa que la Red no debería ser responsable de la seguridad, como señalaba el IETF, pero la gente fue demasiado rígida al respecto durante mucho tiempo y ni siquiera se adoptaron medidas de seguridad que solo tiene sentido incluir dentro de la Red.

Arreglar esto ha sido difícil y algunas veces imposible. El IETF ha hecho propuestas para añadir seguridad al BGP y así prevenir ataques desde 1990, pero siempre han sufrido un problema de acción colectiva. Elegir el sistema más seguro solo tiene ventajas cuando suficientes redes lo hacen. Los pioneros reciben un beneficio mínimo por su arduo trabajo, por lo que el incentivo es absurdo. No tiene mucho sentido que un proveedor de servicios sea el primero en adoptar esta tecnología, ya que paga el coste, pero no obtiene ningún provecho.[25] Tiene mucho más sentido esperar y dejar que sean otros los que lo hagan antes. El resultado, por supuesto, es lo que estamos viendo: veinte años después de empezar a hablar sobre el problema, seguimos sin solución.

Hay otros ejemplos similares. DNSSEC es una actualización que resolvería los problemas de seguridad con el protocolo del sistema de nombres de dominio. Tampoco hay seguridad en el protocolo existente, pero sí todo tipo de formas para atacar al sistema, aunque, igual que con el protocolo de frontera, han pasado veinte años desde que la comunidad tecnológica desarrolló una solución que aún no se ha implementado porque requiere que la mayoría de los sitios la adopten antes de que alguien vea beneficios.[26]

LA EXTENSIBILIDAD DE LOS ORDENADORES SIGNIFICA QUE TODO PUEDE USARSE CONTRA NOSOTROS

Recuerda un teléfono antiguo, parecido al que tus padres o abuelos habrán tenido en sus hogares. Ese objeto fue diseñado y fabricado como un teléfono, y eso es todo lo que hizo y lo que pudo hacer. Compáralo con el teléfono que llevas en tu bolsillo en la actualidad. No es un teléfono; en realidad, es un ordenador que ejecuta una aplicación de teléfono. Y, como sabes, puede hacer mucho mucho más: puede ser un teléfono, una cámara, un sistema de mensajería, un lector de libros, una ayuda para la navegación y un millón de cosas más. «Hay una aplicación para eso» no tendría ningún sentido para un

teléfono antiguo, pero es algo obvio para un ordenador que hace llamadas telefónicas.

De manera similar, en los siglos posteriores a que Johannes Gutenberg inventara la imprenta, alrededor de 1440, la tecnología mejoró considerablemente, aunque seguía tratándose del mismo artefacto mecánico, y luego electromecánico. A lo largo de esos siglos una imprenta era solo una imprenta. No importa lo duro que lo hubiera intentado su operador, no podía utilizarse para hacer cálculos, reproducir música o pesar pescados. Tu antiguo termostato era un aparato electromecánico que detectaba la temperatura y activaba o desactivaba el circuito como respuesta; ese circuito se conectó a tu caldera, lo que le dio al termostato la capacidad de encender y apagar la calefacción: eso es todo lo que podía hacer. Y tu vieja cámara solo podía sacar fotos.

Todas esas máquinas son ahora ordenadores y, como tales, pueden programarse para hacer casi cualquier cosa. Hace poco, unos piratas informáticos demostraron este hecho programando una impresora Canon Pixma,[27] un termostato Honeywell Prestige[28] y una cámara digital Kodak[29] para jugar al juego de ordenador Doom.

Cuando cuento esta anécdota desde el escenario en las conferencias sobre tecnología que doy, todos se ríen de estos dispositivos nuevos de IoT jugando a un juego de ordenador que tiene veinticinco años…, pero nadie se sorprende. Son ordenadores, por supuesto que pueden programarse para jugar a Doom.

Es diferente cuando le cuento la anécdota a un público no técnico. Nuestro modelo mental sobre las máquinas es que solo pueden hacer una cosa, y, si están rotas, no pueden. Pero los ordenadores de propósito general actúan más como personas: pueden hacer casi cualquier cosa.

Los ordenadores son extensibles. Cuando todo se convierta en un ordenador, esta propiedad de extensibilidad se aplicará a todo, lo cual tiene tres ramificaciones cuando hablamos de seguridad.

Una, los sistemas extensibles son difíciles de proteger porque los diseñadores no pueden anticipar cada configuración, condición, aplicación, uso, etc. Esto es una verdadera justificación de su complejidad, por lo que volveremos a este punto dentro de poco.

Dos, los sistemas extensibles no pueden limitarse de forma externa. Es fácil construir un reproductor de música mecánico que solo reproduzca música de cintas magnéticas almacenadas en una carcasa física particular, o una cafetera que solo use cápsulas desechables con una forma determinada,

pero esas limitaciones físicas no se traducen al mundo digital. Lo que esto significa es que la protección de copias, conocida como *administración de derechos digitales* o DRM (por sus siglas en inglés), es básicamente imposible. Como hemos aprendido de las experiencias de las industrias de la música y el cine en las últimas dos décadas, no podemos impedir que las personas hagan y reproduzcan copias no autorizadas de archivos digitales.

De manera más general, un sistema de software no puede restringirse, porque el software usado para ello puede ser rediseñado, reescrito o revisado. Así como es imposible crear un reproductor de música que se niegue a reproducir archivos pirateados, es imposible crear una impresora 3D que se niegue a imprimir partes de armas. Claro, es fácil evitar que una persona normal haga cualquiera de estas cosas, pero es imposible detener a un experto, y una vez que el experto escribe un software para eludir los controles existentes, todos los demás pueden hacerlo también; además, no lleva mucho tiempo: incluso los mejores sistemas de DRM no duran más de veinticuatro horas.[30] Hablaremos de nuevo sobre esto en el capítulo 11.

Tres, la extensibilidad significa que cada ordenador puede actualizarse con funciones adicionales en el software. Estas nuevas funciones pueden incluir inseguridades por accidente, ya que es probable que sus características no se anticipasen en el diseño original y que contengan vulnerabilidades. Pero, lo que es más importante, los atacantes también pueden añadir nuevas funciones. Cuando alguien piratea tu ordenador e instala malware, está introduciendo nuevas funciones, unas que no pediste y que no querías, y que actúan en contra de tus intereses, pero son funciones y pueden, al menos en teoría, instalarse en cada uno de los ordenadores que hay en el mundo.

Las puertas traseras (*backdoors*) también son funciones adicionales en un sistema. Usaré mucho este concepto en el libro, así que vale la pena hacer una pausa para definirlo. Es un antiguo término de criptografía y suele hacer referencia a cualquier mecanismo de acceso diseñado deliberadamente para omitir las medidas de seguridad normales de un sistema informático.[31] A menudo es secreto (y se incluye sin tu conocimiento y consentimiento), pero no tiene por qué serlo. Cuando el FBI le exige a Apple que ofrezca una manera de evitar el cifrado en un iPhone, lo que el organismo está exigiendo es una puerta trasera;[32] cuando los investigadores detectan una contraseña de código duro (*hard code*) en los cortafuegos de Fortinet, encuentran una puerta trasera,[33] y cuando la empresa china Huawei inserta un mecanismo de acceso secreto en sus rúters de Internet, ha instalado una puerta trasera. Desarrollaremos esta cuestión con mayor profundidad en el capítulo 11.

Todos los ordenadores pueden estar infectados con malware y controlarse con ransomware; todos pueden ser secuestrados por una *botnet* (una red de dispositivos infectados con malware que se controla a distancia)[34] y también borrarse de forma remota. La función prevista del ordenador integrado, o el dispositivo del IoT en el que se construye, no hace ninguna diferencia. Los atacantes pueden explotar los dispositivos de IoT de todas las formas en las que explotan los ordenadores de sobremesa y los portátiles en la actualidad.

LA COMPLEJIDAD DE LOS SISTEMAS INFORMATIZADOS SIGNIFICA QUE EL ATAQUE ES MÁS FÁCIL QUE LA DEFENSA

Hoy en día en Internet los atacantes tienen una ventaja sobre los defensores.

Esto no es inevitable. Históricamente, la ventaja fluctúa entre el ataque y la defensa durante períodos de décadas y siglos. La historia de la guerra lo ilustra muy bien, ya que diferentes tecnologías, como ametralladoras y tanques, cambiaron la ventaja de una manera u otra. Pero hoy, con los ordenadores e Internet, el ataque es más fácil que la defensa, y es probable que siga siendo así en el futuro inmediato.[35]

Hay muchas razones para esto, aunque la más importante es la complejidad de estos sistemas. La complejidad es el peor enemigo de la seguridad.[36] Cuanto más complejo es un sistema, menos seguro es. Y nuestros miles de millones de ordenadores, cada uno con sus decenas de millones de líneas de código,[37] conectados a Internet, con sus billones de páginas web y sus desconocidos zettabytes de datos, constituyen las máquinas más complejas que la humanidad ha construido.

Más complejidad significa más personas involucradas, más partes, más interacciones, más capas de abstracción, más errores en el proceso de diseño y desarrollo, más dificultades en las pruebas, más recovecos en el código, donde las inseguridades pueden esconderse.

A los expertos en seguridad informática les gusta hablar sobre la superficie de ataque de un sistema: todos los puntos posibles a los que un atacante podría apuntar y que deben protegerse.[38] Un sistema complejo significa una gran superficie de ataque y, por tanto, una gran ventaja para un posible atacante. El atacante solo tiene que encontrar una vulnerabilidad —una vía no segura para atacar— y elegir el momento y el método de ataque; también puede atacar de forma constante hasta que tenga éxito. Al mismo tiempo, el defensor tiene que proteger la superficie de ataque de todos los

ataques posibles todo el tiempo. Y, mientras que el defensor tiene que ganar todas las veces, al atacante le basta con tener suerte una vez. No es en absoluto una batalla justa, y el coste de atacar un sistema es solo una pequeña parte del coste de defenderlo.

La complejidad ayuda en gran parte a explicar por qué la seguridad informática sigue siendo tan difícil, incluso aunque las tecnologías de seguridad mejoren. Cada año hay ideas, resultados de investigación y productos y servicios nuevos, pero al mismo tiempo, cada año, el aumento de la complejidad da como resultado nuevas vulnerabilidades y ataques. Estamos perdiendo terreno hasta con las mejoras.

También significa que los usuarios a menudo se equivocan en la seguridad. Los sistemas complejos suelen tener muchas opciones, lo que hace que sean difíciles de usar de forma segura; por lo general, no se cambian las contraseñas predeterminadas o se configura de forma incorrecta el control de acceso a los datos en la nube.[39] En 2017, la Universidad de Stanford culpó de la exposición de miles de registros de estudiantes y del personal a una mala configuración de los permisos.[40] Existen muchas historias similares.

Hay otras razones, aparte de la complejidad, por las que el ataque es más fácil que la defensa. Los atacantes tienen la ventaja del primer movimiento, junto con una agilidad natural de la que a menudo carecen los defensores. No suelen tener que preocuparse por las leyes, ni por la moral o la ética convencionales, y pueden hacer uso más rápido de las innovaciones técnicas. Debido a la falta de incentivos actuales para mejorar, somos terribles en la seguridad proactiva. Rara vez tomamos medidas preventivas de seguridad; solo cuando ocurre un ataque. Los atacantes también tienen algo que ganar, mientras que la defensa suele suponer un gasto en el negocio que las empresas buscan minimizar (y muchos de sus ejecutivos todavía no creen que puedan llegar a ser un objetivo). Más ventajas para el atacante.

Esto no significa que la defensa sea inútil, solo que es difícil y cara. Por supuesto, es más fácil si el atacante es un criminal solitario a quien pueda convencerse para que cambie su objetivo, pero siempre habrá un atacante lo bastante capacitado, financiado y motivado. Si hablamos de operaciones cibernéticas de los Estados nación, podemos citar al antiguo director adjunto de la NSA Chris Inglis, quien lo expresó de la siguiente forma: «Si fuéramos a dar los resultados para lo cibernético de la manera que lo hacemos en el fútbol americano, la cuenta sería de 462 a 456 en el minuto veinte de juego, es decir, toda la ofensiva»;[41] lo cual es correcto.

Por supuesto, solo porque el ataque sea técnicamente fácil no significa que vaya a generalizarse. El asesinato también es sencillo, pero pocos lo hacen debido a todos los sistemas sociales que identifican, condenan y procesan a los asesinos.[42] En Internet, la persecución es más difícil, porque la atribución es difícil, un tema que analizaremos en el capítulo 3, y porque la naturaleza internacional de los ataques en la Red da como resultado problemas jurisdiccionales complicados.

Internet+ empeorará estas tendencias. Más ordenadores y, sobre todo, más tipos diferentes de ordenadores significarán una mayor complejidad.

EXISTEN NUEVAS VULNERABILIDADES EN LAS INTERCONEXIONES

Internet está lleno de características emergentes y consecuencias no deseadas. Es decir, incluso los expertos no entienden tan bien como nos gustaría creer cómo interactúan entre sí las distintas partes de Internet, y con frecuencia nos sorprende cómo funcionan las cosas en realidad. Esto también sirve para las vulnerabilidades.

Cuanto más conectemos las cosas, más afectarán las vulnerabilidades de un sistema a otros sistemas. Tres ejemplos:

1. En 2013, unos delincuentes piratearon la red de la empresa Target y robaron los datos de setenta millones de clientes y de cuarenta millones de tarjetas de crédito/débito. Los delincuentes obtuvieron acceso a la red de Target porque primero pudieron robar las credenciales de inicio de sesión de uno de los proveedores de calefacción y aire acondicionado de la empresa.[43]
2. En 2016, piratas informáticos recolectaron millones de ordenadores IoT (rúters, DVR, cámaras web, etc.) en una red de robots zombis masiva (botnet) llamada Mirai. Luego utilizaron esa misma red para lanzar un ataque distribuido de denegación de servicio (un ataque DdoS, por sus siglas en inglés) contra Dyn, un proveedor de nombres de dominio. Dyn proporciona una función crítica de Internet a muchos de los principales sitios de la Red, así que, cuando este cayó, docenas de páginas web populares, como Reddit, BBC, Yelp, PayPal o Etsy, se quedaron sin conexión.[44]
3. En 2017, piratas informáticos penetraron en una red sin nombre de casinos a través de una pecera conectada a Internet y robaron los datos.

[45]

Los sistemas pueden afectar a otros sistemas de maneras imprevistas y potencialmente dañinas. Lo que podría parecer inofensivo para los diseñadores de un sistema en particular se vuelve perjudicial cuando se combina con algún otro. Las vulnerabilidades en un sistema caen en cascada en otros y el resultado es una vulnerabilidad que nadie se esperaba. Así es como pueden suceder cosas como el desastre nuclear de Three Mile Island, la explosión del transbordador espacial *Challenger* o el apagón de 2003 en Estados Unidos y Canadá.

Esto tiene dos repercusiones. Por un lado, las interconexiones nos dificultan descubrir qué sistema está fallando y, por otro, es posible que en realidad ningún sistema individual esté fallando, sino que la causa podría ser la interacción insegura de dos sistemas individualmente seguros. En 2012, comprometieron la cuenta de Amazon del periodista Mat Honan, lo que permitió acceder a su cuenta de Apple, que dio acceso a su cuenta de Gmail, y esto, a su vez, permitió que entraran en su cuenta de Twitter.[46] La trayectoria particular del ataque es importante: algunas de las vulnerabilidades no se encontraban en los sistemas individuales y solo se volvieron explotables cuando se utilizaron en conjunto.

Hay otros ejemplos: una vulnerabilidad en los frigoríficos inteligentes de Samsung dejó las cuentas de Gmail de los usuarios abiertas a ataques;[47] el giroscopio de tu iPhone, colocado para detectar movimientos y orientación, es lo bastante sensible como para captar vibraciones acústicas, por lo que puede escuchar conversaciones,[48] y el software antivirus que vende Kaspersky robó por accidente (o a propósito) secretos del Gobierno de Estados Unidos.[49]

Si cien sistemas interactúan entre sí, representan unas cinco mil interacciones y cinco mil vulnerabilidades potenciales resultantes de esas interacciones. Si trescientos sistemas interactúan entre ellos, tenemos 45.000 interacciones. Mil sistemas suponen medio millón de interacciones. La mayoría de ellas serán inofensivas o poco interesantes, pero algunas tendrán consecuencias muy perjudiciales.

LOS ORDENADORES FALLAN DE DIFERENTES MANERAS

Los ordenadores no fallan de la misma manera que las cosas normales. Son vulnerables de tres importantes y diferentes maneras.

Una: la distancia no importa. En el mundo real nos preocupa la seguridad contra el atacante común. No compramos una cerradura de puerta para que el mejor ladrón del mundo no se acerque, sino para alejar a los ladrones habituales que quizá deambulen por nuestro vecindario. Tengo una casa en Cambridge, pero no me importa si hay una ladrona superbuena en Canberra; no va a atravesar el océano para robar en mi casa. Sin embargo, en Internet, una pirata informática de Canberra puede hackear mi red doméstica con la misma facilidad que una al otro lado de mi calle.

Dos: la posibilidad de atacar ordenadores no tiene relación con el conocimiento para hacerlo. El software encierra el conocimiento. Esa pirata informática superhábil de Canberra puede convertir su saber hacer en un software, automatizar su ataque y hacer que se ejecute mientras duerme, y luego puede dárselo a todo el mundo. De aquí proviene el término *script kiddie*: alguien con unas habilidades mínimas, pero con un software poderoso. Si el mejor ladrón del mundo pudiera distribuir con libertad una herramienta que permitiera al ladrón común entrar en tu casa, estarías más preocupado por la seguridad de tu hogar.

Esto sucede todo el tiempo en Internet. El atacante que creó la red zombi Mirai lanzó su código al mundo y en una semana había una docena de herramientas de ataque que estaban utilizándolo.[50] Este es un ejemplo de lo que llamamos malware: gusanos, virus y *rootkits*[51] que brindan capacidades enormes a los atacantes no cualificados. Los hackers pueden comprar *rootkits* en el mercado negro y contratar ransomware como si fuera un servicio.[52] Algunas compañías europeas, como HackingTeam y Gamma International, venden herramientas de ataque a Gobiernos más pequeños de todo el mundo.[53] El Servicio Federal de Seguridad de Rusia tenía a un ciudadano kazajo-canadiense de veintiún años, Karim Baratov, realizando ataques de suplantación de identidad que llevaron al exitoso ataque del Comité Nacional Demócrata de 2016. El malware fue creado por el experto hacker Alexsey Belan.[54]

Tres: los ordenadores fallan todos a la vez o ninguno. La *rotura de clase* es un concepto de seguridad informática,[55] un tipo particular de vulnerabilidad que rompe no solo un sistema, sino toda una clase de ellos. Los ejemplos pueden ser una vulnerabilidad de un sistema operativo que le permita a un atacante tomar el control remoto de cada ordenador que lo ejecuta o una vulnerabilidad en las grabadoras de vídeo digitales y cámaras web habilitadas para Internet que permita a un atacante reclutar esos dispositivos en una red zombi.

El documento nacional de identidad de Estonia sufrió un rotura de clase en 2017: un error criptográfico obligó al Gobierno a suspender 760.000 documentos utilizados para todo tipo de servicios gubernamentales, algunos en entornos de alta seguridad.[56]

Los riesgos se agravan por la elección unánime de software y hardware. Casi todos nosotros tenemos uno de los tres sistemas operativos para ordenadores y uno de los dos sistemas operativos móviles. Más de la mitad de nosotros usamos el navegador web Chrome; la otra mitad, uno de los otros cinco. La mayoría de nosotros utilizamos Microsoft Word para procesamiento de textos y Excel para hojas de cálculo. Casi todos nosotros leemos PDF, miramos JPEG, escuchamos MP3 y vemos archivos de vídeo AVI. Casi todos los dispositivos del mundo se comunican con los mismos protocolos de Internet TCP/IP. Y los estándares informáticos básicos no son la única fuente de elecciones coincidentes. Según un estudio de DHS de 2011, el GPS es esencial para once de los quince sectores de la infraestructura.[57] Las roturas de clase en ellos, así como en muchas otras funciones y protocolos comunes, pueden afectar con facilidad a millones de dispositivos y de personas. En estos momentos, el IoT está mostrando más diversidad, pero no durará, a menos que se modifiquen algunas políticas económicas bastante básicas. En el futuro solo habrá unos pocos procesadores de IoT, sistemas operativos de IoT, controladores y protocolos de comunicaciones.

Las roturas de clase conducen a gusanos, virus y otros programas maliciosos. Piensa en «ataca una vez, impacta a muchos». Hemos concebido el fraude electoral como una serie de individuos no autorizados intentando votar, no como parte de la manipulación remota de una única persona o por parte de una organización con máquinas de votación conectadas a Internet o listas de votantes en línea. Pero así es como fallan los sistemas informáticos: alguien hackea las máquinas.

Piensa en un carterista: le ha llevado tiempo desarrollar su habilidad, cada víctima es un nuevo trabajo, y el éxito en un robo no lo garantiza en el siguiente. Las cerraduras electrónicas de las puertas como las que hay ahora en las habitaciones de los hoteles tienen diferentes grados de vulnerabilidad. Un atacante puede encontrar un error en el diseño que le permita crear una tarjeta de acceso que abra todas las puertas. Si publica su software de ataque, no solo él, sino cualquiera, podrá saltarse todos los bloqueos. Y, si esas cerraduras están conectadas a Internet, los atacantes podrían abrir las puertas de forma remota (incluso todas al mismo tiempo). Eso es una rotura de clase.

Esto le sucedió en 2012 a Onity, una compañía que fabrica cerraduras electrónicas para más de cuatro millones de habitaciones de hotel de cadenas como Marriott, Hilton e InterContinental.[58] Un dispositivo casero les permitió a los hackers eliminar los bloqueos en segundos. Alguien lo descubrió, y las instrucciones sobre cómo construir el dispositivo se difundieron con rapidez. A Onity le costó meses darse cuenta de que lo habían pirateado y, como no había manera de reparar el sistema (hablaremos de esto en el capítulo 2), las habitaciones de los hoteles fueron vulnerables durante meses e incluso años después.[59]

Las roturas de clase no son un concepto nuevo en la gestión de riesgos. Es la diferencia entre los robos en el hogar y los incendios, que ocurren ocasionalmente en diferentes casas de un vecindario a lo largo del año, e inundaciones y terremotos, que pueden suceder a todos en el mismo vecindario o a nadie. Pero los ordenadores tienen partes de ambas cosas al mismo tiempo y también aspectos del modelo de riesgos para la salud pública.

Esto cambia la naturaleza de los fallos de seguridad y altera por completo la forma en la que debemos defendernos. No nos preocupa la amenaza que representa el atacante común, sino el individuo más extremo, que puede arruinarlo todo.

LOS ATAQUES SIEMPRE SON MEJORES, MÁS FÁCILES Y MÁS RÁPIDOS

El estándar de encriptación de datos (DES, por sus siglas en inglés) es un algoritmo de cifrado de la década de los setenta. Su seguridad fue diseñada a propósito para ser lo bastante fuerte como para resistir los ataques entonces factibles, pero no más que eso. En 1976, los expertos en criptografía estimaron que la construcción de una máquina para romper el DES costaría veinte millones de dólares.[60] En mi libro de 1995, *Applied Cryptography* (*Criptografía aplicada*), estimé que el coste se había reducido a un millón.[61] En 1998, Electronic Frontier Foundation construyó una máquina personalizada por 250.000 dólares para romper el cifrado DES en menos de un día.[62] Hoy puedes hacerlo desde tu portátil.

En otro ámbito, en los años noventa, los móviles se diseñaron para confiar automáticamente en las torres de telefonía sin ningún sistema de autenticación. Esto se debía a que la autenticación era difícil, como también lo era instalar torres falsas. Avanzada media década, las torres falsas de telefonía Stingray se convirtieron en una herramienta de vigilancia secreta del

FBI.[63] Pasada otra media década, configurar una torre falsa era tan fácil que los hackers lo demuestran en el escenario durante sus conferencias.[64]

De manera parecida, la velocidad cada vez mayor de los ordenadores los ha hecho exponencialmente más rápidos adivinando contraseñas mediante la fuerza bruta: probar contraseñas hasta encontrar la correcta. Mientras tanto, la longitud y la complejidad típicas de las contraseñas que el ciudadano medio desea y puede recordar se ha mantenido constante. El resultado son contraseñas que eran seguras hace diez años, y que hoy son inseguras.[65]

Escuché por primera vez esta máxima de un empleado de la NSA: «Los ataques siempre son mejores, nunca empeoran». Los ataques se vuelven más rápidos, más baratos y más fáciles. Lo que hoy es teórico mañana se convierte en práctico. Y, debido a que nuestros sistemas de información permanecen activos mucho más tiempo de lo planeado, tenemos que prepararnos para defendernos de atacantes que utilicen tecnología del futuro.

Los atacantes también aprenden y se adaptan; esto es lo que hace que la seguridad sea diferente de la protección. Los tornados son un problema de protección, y podríamos hablar sobre diferentes formas de defensa contra ellos y su relativa eficacia y preguntarnos cómo los avances tecnológicos futuros podrían protegernos mejor de su capacidad destructiva, pero, independientemente de lo que decidamos hacer o no, sabemos que los tornados nunca se adaptarán a nuestras defensas ni cambiarán su comportamiento; solo son tornados.

Los adversarios humanos son diferentes: creativos e inteligentes, cambian de táctica, inventan cosas nuevas y se adaptan todo el tiempo. Los atacantes examinan nuestros sistemas, siempre buscando roturas de clase; cuando alguno de ellos encuentra una, la explotará una y otra vez hasta que se solucione la vulnerabilidad. Una medida de seguridad que protege las redes hoy podría no funcionar mañana, porque los atacantes habrán descubierto cómo sortearla.

Todo esto significa que la experiencia va cuesta abajo. Las capacidades militares secretas de ayer se convierten en las tesis doctorales de hoy y en las herramientas de piratería de mañana. El criptoanálisis diferencial fue una de esas capacidades y fue descubierto por la NSA en algún momento antes de 1970. En la década de los setenta, los matemáticos de IBM lo descubrieron de nuevo mientras diseñaban el DES (estándar de cifrado de datos, por sus siglas en inglés).[66] La NSA catalogó el descubrimiento de IBM, pero la técnica fue redescubierta por criptógrafos académicos a finales de los años ochenta.[67]

La defensa siempre está en movimiento. Lo que ayer funcionaba podría no hacerlo hoy y es casi seguro que no funcione mañana.

02

PARCHEAR FALLA COMO PARADIGMA DE SEGURIDAD

EXISTEN DOS PARADIGMAS BÁSICOS en la seguridad. El primero proviene del mundo real de las tecnologías peligrosas: los automóviles, los aviones, las farmacéuticas, la arquitectura, la construcción y las herramientas médicas. Es la forma tradicional en la que diseñamos y puede resumirse mejor con la expresión «hacerlo bien desde el principio». Este es el mundo de las pruebas rigurosas, de las certificaciones de seguridad y de los ingenieros con licencia; es decir, un proceso lento y caro. Piensa en todas las pruebas de seguridad que Boeing realiza para su nuevo avión o en las de cualquier compañía farmacéutica antes de lanzar un nuevo medicamento al mercado. También es el mundo de los cambios lentos y costosos, porque cada uno tiene que pasar por el mismo proceso.

Hacemos esto porque el coste de hacerlo mal es inmenso. No queremos que los edificios se derrumben sobre nosotros, ni que los aviones se caigan del cielo, ni que miles de personas mueran por los efectos secundarios de un producto farmacéutico o por la interacción de un medicamento. Y, aunque no podemos eliminar por completo todos esos riesgos, podemos mitigarlos haciendo un montón de trabajo inicial.

El paradigma de seguridad alternativo proviene del mundo del software de rápido movimiento y de libre desplazamiento, altamente complejo y hasta ahora bastante inofensivo. Su lema es «asegúrate de que tu seguridad sea ágil» o, en la jerga de Facebook, «muévete rápido y rompe cosas».[1] En este modelo intentamos asegurarnos de que nuestros sistemas puedan actualizarse con rapidez cuando se descubren vulnerabilidades de seguridad. Tratamos de construir sistemas que sobrevivan a un ataque, se recuperen de él o lo mitiguen y se adapten a las amenazas cambiantes. Pero sobre todo construimos sistemas que podemos parchear rápida y eficientemente. Cabe discutir si de verdad alcanzamos estos objetivos, aunque aceptamos los problemas porque el coste de hacerlo mal no es tan grande.

En la seguridad de Internet+ estos dos paradigmas están en conflicto: en tu coche, tus electrodomésticos, en los dispositivos médicos computarizados, los termostatos domésticos, las máquinas de votación informatizadas, los sistemas de control de tráfico y en nuestras plantas químicas, presas y centrales eléctricas. Chocan uno contra el otro una y otra vez, y las apuestas son cada vez más altas porque los errores pueden afectar a la vida y la propiedad.

Parchear es algo que hacemos todo el tiempo con nuestro software, (generalmente lo llamamos *actualizar*) y es el mecanismo principal que tenemos para mantener nuestros sistemas seguros. Es importante comprender cómo funciona (y no funciona) y cómo lo hará en el futuro para apreciar los desafíos de seguridad a los que nos enfrentamos.

Hay vulnerabilidades ocultas en cada aplicación que permanecen inactivas durante meses y años, y otras nuevas las descubren de forma constante empresas, Gobiernos, investigadores independientes y ciberdelincuentes. Preservamos nuestra seguridad mediante 1) descubridores que revelan una vulnerabilidad al proveedor de software y al público, 2) proveedores que emiten rápidamente un parche de seguridad para corregir la vulnerabilidad y 3) usuarios que instalan ese parche.

Nos ha llevado mucho tiempo llegar hasta aquí. A principios de 1990, los investigadores les revelaban las vulnerabilidades solo a los proveedores, quienes respondían básicamente no haciendo nada o a lo mejor solucionando los problemas años más tarde. Luego los investigadores comenzaron a anunciar que habían encontrado una vulnerabilidad tratando de que los proveedores hicieran algo al respecto, pero estos minimizaban los errores, declaraban sus ataques como *teóricos* y, por lo tanto, sin ninguna razón por la cual preocuparse y los amenazaban con acciones legales. Y seguían sin arreglar nada. La única solución que impulsó a los proveedores a actuar fue que los investigadores publicaran detalles sobre la vulnerabilidad. Hoy, los investigadores advierten primero a los proveedores de software cuando encuentran una vulnerabilidad y luego publican los detalles. La publicación se ha convertido en aquello que motiva a los proveedores a lanzar parches de seguridad con celeridad, así como los medios para que los investigadores aprendan unos de otros y se les reconozca su trabajo; esto mejora aún más la seguridad al proporcionar a otros investigadores conocimiento e incentivos. Si oyes el término *divulgación responsable*, están hablando de este proceso.[2]

Muchos investigadores encuentran y divulgan de manera responsable las vulnerabilidades, desde hackers solitarios hasta investigadores académicos e

ingenieros corporativos. Las compañías ofrecen recompensas a los hackers que les muestran vulnerabilidades en lugar de publicarlas o usarlas para cometer delitos. Google tiene un equipo completo llamado Project Zero dedicado a encontrar vulnerabilidades en los softwares de uso común, tanto de dominio público como de propiedad exclusiva.[3] Podríamos discutir las motivaciones de estos investigadores (muchos de ellos están a favor de la publicidad o de la ventaja competitiva), pero no sus resultados. A pesar del flujo interminable de vulnerabilidades, cualquier programa de software se vuelve más seguro conforme estas se descubren y se solventan.[4]

Sin embargo, ni vivimos felices ni comemos perdices. Hay varios problemas con el sistema de búsqueda y de parcheo, muchos de los cuales se ven exacerbados por Internet+. Veámoslo en términos de todo el ecosistema en orden cronológico inverso: la investigación de vulnerabilidades, la revelación de estas al fabricante, la redacción, la publicación de parches y su instalación.

INSTALAR PARCHES

Recuerdo los primeros años en que los usuarios, especialmente en las redes corporativas, dudaban de la instalación de parches. A menudo estos se testaron mal y con demasiada frecuencia rompieron más de lo que repararon. Esto les ocurrió a todos los que lanzaron software: proveedores de sistemas operativos, grandes proveedores de software, etc., pero ha cambiado con los años. Las grandes organizaciones de sistemas operativos, en particular Microsoft, Apple y Linux, mejoraron mucho las pruebas de sus parches antes de lanzarlos y, a medida que las personas se sintieron más cómodas con estos, los instalaron más rápido y con más frecuencia. Al mismo tiempo, los proveedores comenzaron a hacer que los parches fueran más fáciles de instalar.

No obstante, no todo el mundo parchea sus sistemas. La regla de oro de la industria es que una cuarta parte de nosotros los instalamos el día que aparecen, otra cuarta parte dentro del mismo mes, otra cuarta parte dentro del año y otra cuarta parte nunca lo hace. La tasa de actualización es aún más baja para los sistemas militares, industriales y de atención médica debido a la especialización del software: aumenta la probabilidad de que un parche rompa alguna funcionalidad crítica.

Quienes utilizan copias pirateadas de software a menudo no pueden obtener actualizaciones, algunas personas no quieren que las molesten o se

olvidan y otras no parchean porque están cansadas de que los proveedores incluyan funciones y software no deseados en las actualizaciones.[5] Algunos sistemas del IoT son más difíciles de actualizar. ¿Con qué frecuencia actualizas el software en tu rúter, frigorífico o microondas? Supongo que nunca. Y no, no se actualizan solos.

Tres ejemplos de 2017 ilustran el problema: Equifax fue pirateado porque no instaló en su servidor web Apache una actualización disponible dos meses antes;[6] el malware WannaCry fue un azote mundial, aunque solo afectó a los sistemas de Windows sin parches, y la red zombi Amnesia IoT hizo uso de una vulnerabilidad en las grabadoras de vídeo digital revelada y reparada un año antes, pero no pudieron parchearse las máquinas existentes.[7]

La situación es peor para los ordenadores integrados en dispositivos del IoT. En muchos sistemas, tanto de bajo coste como caros, los usuarios tienen que descargar e instalar a mano las actualizaciones relevantes. A menudo el proceso de aplicación de parches es tedioso y complicado, y está más allá de la habilidad del usuario promedio. A veces los ISP (proveedores de acceso a Internet) tienen la capacidad de parchear remotamente cosas como rúters y módems, aunque es poco común.[8] Peor aún, no hay forma alguna de parchear muchos dispositivos integrados. En este momento la única forma de actualizar el firmware en tu DVR hackeable es tirarlo y comprar uno nuevo.[9]

En el extremo inferior del mercado, tenemos como resultado cientos de millones de dispositivos, que llevan en Internet los últimos cinco o diez años, sin parches e inseguros. En 2010, un investigador de seguridad analizó treinta rúters domésticos y pudo acceder a la mitad de ellos, incluidos algunos de las marcas más populares y comunes.[10] Las cosas no han mejorado desde entonces.[11]

Los hackers empiezan a darse cuenta. El malware DNS Changer ataca tanto a los rúters domésticos como a los ordenadores.[12] En Brasil, en 2012, 4,5 millones de rúters DSL se vieron comprometidos con fines de fraude financiero.[13] En 2013, un gusano de Linux se dirigió a rúters, cámaras y otros dispositivos integrados.[14] En 2016, la red zombi Mirai utilizó vulnerabilidades en grabadoras de vídeo digitales, cámaras web y rúters:[15] explotó errores de seguridad de novatos, como el uso de contraseñas predeterminadas.[16]

La dificultad de parchear también afecta a los costosos dispositivos del IoT, que uno esperaría que estuvieran mejor diseñados. En 2015, Chrysler retiró 1,4 millones de vehículos para reparar la vulnerabilidad de seguridad con la que he abierto este libro;[17] la única forma de actualizar era que

Chrysler le enviara a cada propietario un USB para conectarlo a un puerto en el panel de mando del vehículo. En 2017, los laboratorios Abbott les comunicaron a 465.000 pacientes con marcapasos que tenían que acudir a una clínica autorizada para una actualización de seguridad crítica;[18] al menos no tuvieron que abrirles el pecho.

Es probable que este sea un problema temporal, por lo menos en los dispositivos más caros. Las industrias que no estén acostumbradas a parchear aprenderán cómo hacerlo y las empresas que venden caros equipos con ordenadores integrados aprenderán a diseñar sus sistemas para que se actualicen de forma automática. Compara Tesla con Chrysler: Tesla envía actualizaciones y parches a los vehículos automáticamente y actualiza los sistemas durante la noche. Kindle hace lo mismo: los propietarios no tienen control sobre el proceso de aplicación de parches y, por lo general, no saben que sus dispositivos se actualizan.[19]

ESCRIBIR Y PUBLICAR PARCHES

Los proveedores pueden tardar en lanzar parches de seguridad. Una encuesta realizada en 2016 encontró que aproximadamente el 20 % de todas las vulnerabilidades (y el 7 % de ellas en las cincuenta aplicaciones principales) no tenían una actualización disponible el mismo día en que estas se revelaron.[20] (Para ser justos, esto supone una mejora con respecto a los años anteriores. En 2011, no había parche disponible para un tercio de todas las vulnerabilidades el día de su divulgación). Peor aún, solo un 1 % adicional se reparó en menos de un mes tras conocerse las vulnerabilidades, lo que indica que, si un proveedor no lanza un parche de inmediato, es probable que no llegue pronto. Los usuarios de Android, por ejemplo, con frecuencia tienen que esperar meses desde que Google emite un parche hasta que los fabricantes de sus teléfonos lo ponen a su disposición;[21] el resultado es que la mitad de los teléfonos con Android no se han actualizado en más de un año.[22]

Los parches tampoco son tan fiables como nos gustaría que fuesen: a veces rompen los sistemas que se supone que deben arreglar. En 2014, un parche de iOS dejó a algunos usuarios sin capacidad para recibir señal de conexión.[23] En 2017, un parche defectuoso en las cerraduras electrónicas para puertas de LockState bloqueó los dispositivos y no permitía a los usuarios abrir ni cerrar sus puertas.[24] En 2018, como respuesta a las vulnerabilidades de Spectre y Meltdown en las CPU de los ordenadores,

Microsoft sacó un parche para su sistema operativo que bloqueó algunos ordenadores.[25] Y hay mas ejemplos.[26]

Si nos centramos en los sistemas integrados y dispositivos IoT, la situación es mucho más grave. Nuestros ordenadores y teléfonos inteligentes son tan seguros porque hay equipos de ingenieros de seguridad dedicados a escribir parches. Esas compañías pueden apoyar equipos tan grandes porque ganan una gran cantidad de dinero por su software, ya sea directa o indirectamente, y, en parte, compiten por la seguridad. Esto no ocurre en sistemas integrados, como grabadoras de vídeo digitales o rúters domésticos; son sistemas que se venden con un margen mucho menor y en cantidades mucho más pequeñas y suelen estar diseñados por terceros en el extranjero. Los equipos de ingeniería se reúnen rápidamente para diseñar los productos, luego se disuelven o construyen algo más. Algunas partes del código pueden ser antiguas y desactualizadas, y reutilizarse una y otra vez. Puede que no haya ningún código fuente disponible, lo que hace que escribir parches sea mucho más difícil. Las compañías involucradas no tienen el presupuesto para hacerlas seguras y no existe ningún aliciente comercial para que lo hagan.

Peor aún, nadie tiene incentivos para parchear el software una vez que se envía. El fabricante del chip está ocupado con la próxima versión, el fabricante del dispositivo está ocupado actualizando su producto para que funcione con el siguiente chip, y el proveedor, cuyo nombre aparece en la caja, es solo un revendedor. Conservar los chips y productos más antiguos no es una prioridad para nadie.

Incluso cuando los fabricantes tienen alicientes hay otro problema. Si existe una vulnerabilidad de seguridad en los sistemas operativos de Microsoft, la empresa debe escribir un parche para cada versión. Mantener muchos sistemas operativos diferentes se vuelve caro, por lo que Microsoft y Apple (y todos los demás) solo soportan unas pocas versiones recientes.[27] Si estás utilizando una versión anterior de Windows o macOS, no obtendrás parches de seguridad, porque las empresas ya no los están creando.

Esto no funcionaría con bienes más duraderos. Podríamos comprar un nuevo DVR cada cinco o diez años y un frigorífico cada veinticinco. Un vehículo que compramos hoy lo conducimos durante toda una década, luego se lo vendemos a otro que lo conduce otra década y esa persona se lo vende a alguien que lo envía a un país del tercer mundo, donde vuelve a revenderse y se usa durante una o dos décadas más. Intenta encender un ordenador Commodore Pet de 1978 o ejecutar el VisiCalc del mismo año, y verás qué sucede; no sabemos cómo mantener el software de hace cuarenta años.

Piensa en una empresa de automóviles. Podrían vender una docena de modelos de vehículos diferentes con una docena de clases distintas de software cada año. Incluso suponiendo que el software se actualice solo cada dos años y que sean compatibles con los vehículos durante solo dos décadas, la compañía necesita tener la capacidad de actualizar de veinte a treinta versiones de software diferentes (para una empresa como Bosch, que suministra piezas de automóviles para muchos fabricantes diferentes, el número sería más cercano a las doscientas). El gasto y el tamaño del almacenaje para los vehículos de prueba y el equipo asociado serían enormes.

Por otro lado, imagina a las empresas de automóviles anunciando que ya no se encargarán de vehículos de más de cinco o diez años: tendría graves consecuencias medioambientales.

Ya estamos viendo los efectos de sistemas tan antiguos que los proveedores dejan de actualizarlos o han cerrado su negocio. Algunas de las organizaciones afectadas por WannaCry seguían usando Windows XP: un sistema operativo de hace diecisiete años que no puede parchearse y que Microsoft dejó de soportar en 2014.[28] Unos 140 millones de ordenadores en todo el mundo aún ejecutan ese sistema operativo,[29] incluida la mayoría de los cajeros automáticos ATM.[30] Un popular sistema de comunicación por satélite que vendía el Grupo Inmarsat ya no tiene parches, a pesar de que tiene importantes problemas de seguridad.[31] El hecho de que las actualizaciones sean tan caras, al requerir mucha especialización, supone una gran traba para los sistemas de control industrial, muchos de los cuales ejecutan software y sistemas operativos desactualizados. Estos sistemas pueden estar en funcionamiento durante muchos años, y no suelen contar con grandes presupuestos de TI asociados.

La certificación agrava el problema. Antes de que todo se convirtiera en un ordenador, los artefactos peligrosos, como automóviles, aviones y dispositivos médicos, tenían que pasar por varios niveles de certificaciones de seguridad para que pudieran venderse. Una vez certificado un producto, este no puede cambiarse sin volver a certificarse. Para un avión, el cambio de una sola línea de código puede costar un millón de dólares y tardar un año.[32] Esto tenía sentido en el mundo analógico, en el que los productos no cambiaban mucho, pero el objetivo de las actualizaciones es permitir que los productos cambien y que lo haga deprisa.

REVELAR VULNERABILIDADES

No todos revelan las vulnerabilidades de seguridad cuando las encuentran, y hay quienes se las guardan con propósitos ofensivos. Los atacantes las usan para penetrar en los sistemas y eso es lo primero que aprendemos de ellos. Se denominan *vulnerabilidades de día cero*, y los proveedores responsables intentan parchearlas rápidamente. Los organismos gubernamentales, como la NSA, el Cibercomando de Estados Unidos y sus equivalentes extranjeros, también mantienen en secreto algunas vulnerabilidades para su uso presente y futuro. Hablaremos mucho más de esto en el capítulo 9, pero por ahora ten en cuenta que cada vulnerabilidad descubierta, y no revelada, aun cuando sea por alguien en quien confiemos, también puede encontrarla otra persona y utilizarla contra ti.

Incluso los propios investigadores que desean revelar las vulnerabilidades que descubren se encuentran con una respuesta fría por parte de los fabricantes de dispositivos. Las nuevas industrias que están entrando en el negocio de los ordenadores (fabricantes de cafeteras y ese tipo de cosas) no tienen experiencia con los investigadores de seguridad, la divulgación responsable y los parches, y se nota. Esta falta de experiencia en seguridad es crítica. Las compañías de software escriben el código como lo hace su competencia principal. Los fabricantes de frigoríficos, o las divisiones de frigoríficos de compañías más grandes, tienen un objetivo principal diferente (presumimos que mantener los alimentos fríos), por lo que escribir software siempre será una actividad secundaria.

De la misma manera que los proveedores de ordenadores de la década de los noventa se jactaban de la inquebrantabilidad de sus sistemas, los fabricantes de IoT niegan cualquier problema y amenazan con emprender acciones legales contra quienes digan lo contrario. El parche de los laboratorios Abbot de 2017 llegó un año después de que la compañía considerase el informe inicial de vulnerabilidad de seguridad *falso y engañoso*, y fue publicado sin dar detalles del ataque.[33] Este tipo de cosas podría no tener importancia para los juegos de ordenador o los procesadores de texto, pero es peligroso para los automóviles, dispositivos médicos y aviones, artefactos que pueden matar a las personas si se explotan sus virus y errores. Pero ¿deberían los investigadores publicar los detalles de todos modos? Nadie sabe cómo se ve la divulgación responsable dentro de este nuevo entorno.

AL FIN, INVESTIGAR LAS VULNERABILIDADES

Para que este ecosistema funcione necesitamos que los investigadores encuentren vulnerabilidades y mejoren la seguridad, pero la llamada Ley de Derechos de Autor de la Era Digital (DMCA, por sus siglas en inglés) lo está bloqueando. Es una ley contra la copia que discutiremos en el capítulo 4 y que incluye una prohibición contra la investigación de seguridad. Técnicamente, la prohibición va contra las características del producto destinadas a la reproducción no autorizada de obras con derechos de autor, pero sus efectos son más amplios. Debido a la ley DMCA, es ilegal la ingeniería inversa: localizar y publicar vulnerabilidades en los sistemas de software que protegen los derechos de autor. Dado que el software puede estar protegido por derechos de autor, los fabricantes han usado en multitud de ocasiones esta ley para acosar y molestar a los investigadores de seguridad que podrían avergonzarlos.

Uno de los primeros ejemplos de esto sucedió en 2001. El FBI arrestó a Dmitry Sklyarov en la conferencia de piratas informáticos DefCon por impartir una charla describiendo cómo omitir el código de cifrado en Adobe Acrobat, diseñado para evitar que las personas copiaran libros electrónicos.[34] También en 2001, HP se valió de la ley para amenazar a los investigadores que publicaron fallos de seguridad en su producto Tru64.[35] En 2011, Activision lo utilizó para cerrar el sitio web público de un ingeniero que investigó el sistema de seguridad de uno de sus videojuegos. Existen muchos ejemplos como estos.[36]

En 2016, la Biblioteca del Congreso (en serio, fue la responsable de esto) añadió una exención a la DMCA para los investigadores de seguridad,[37] aunque está restringida, es temporal y todavía deja mucho espacio para el acoso.[38]

Otras leyes también se utilizan para silenciar las investigaciones. En 2008, el Metro de Boston (MBTA, por sus siglas en inglés) utilizó la Ley de Abuso y Fraude Informático para bloquear una conferencia sobre fallos en sus tarjetas de transporte.[39] En 2013, Volkswagen demandó a los investigadores de seguridad que encontraron vulnerabilidades en el software de sus automóviles, lo que impidió que se divulgaran durante dos años.[40] Y en 2016, la compañía de seguridad de Internet FireEye obtuvo una orden judicial contra la publicación de detalles de vulnerabilidades descubiertas en productos por parte de terceros.[41]

Estos escalofriantes efectos son significativos. Muchos investigadores de seguridad no trabajan para encontrar vulnerabilidades porque podrían demandarlos y no publicar sus resultados. Si eres un joven académico

preocupado por la propiedad, la publicación y evitar demandas, es mejor que no te arriesgues.[42]

Por todas estas razones, el sistema actual de parches será cada vez menos adecuado conforme los ordenadores se integren en más y más cosas. El problema es que no tenemos nada mejor para reemplazarlo.

Esto nos lleva de vuelta a los dos paradigmas con los que comenzaba este capítulo: hacerlo bien desde el principio y solucionar los problemas deprisa cuando surjan.

Esto guarda paralelismos con la industria de desarrollo de software. Utilizamos el término *cascada* para el modelo tradicional del desarrollo de software: primero, vienen los requisitos; luego las especificaciones; después el diseño, y, por último, la implementación y las pruebas de campo.[43] El desarrollo ágil es el modelo más nuevo para el desarrollo de software: crea un prototipo para satisfacer las necesidades básicas de los clientes, analiza los fallos, lo repara deprisa, actualiza los requisitos y las especificaciones, y lo repite una y otra vez.[44] Parece ser una forma mucho mejor de diseñar y desarrollar software, pues puede incorporar requisitos de seguridad, así como de diseño funcional.

Puedes ver la diferencia comparando Microsoft Office con las aplicaciones de tu teléfono inteligente. Las versiones nuevas de la suite ofimática salen una vez cada pocos años —lo que supone un gran esfuerzo de desarrollo de software que da como resultado muchos cambios de diseño y nuevas funciones—, mientras que, por otro lado, es posible que se publiquen versiones nuevas de una aplicación de iPhone cada dos semanas, cada una con pequeños cambios progresivos y, ocasionalmente, nuevas funciones. Microsoft podría usar procesos internos de desarrollo ágil, pero sus novedades son por completo de la vieja escuela.

Necesitamos integrar esos dos paradigmas.[45] No tenemos la habilidad necesaria en ingeniería de seguridad para hacerlo bien desde el principio, por lo que no nos queda más remedio que parchear rápidamente. Pero también tenemos que descubrir cómo mitigar los costes de los fallos inherentes a este paradigma. Debido a la complejidad consustancial a Internet+, necesitamos tanto la estabilidad a largo plazo del primer paradigma como la capacidad reactiva del segundo.

03

SABER QUIÉN ES QUIÉN CADA VEZ ES MÁS DIFÍCIL EN INTERNET

UNA FAMOSA CARICATURA DEL *New Yorker* de 1993 mostraba a dos perros hablando entre ellos con la leyenda «En Internet nadie sabe que eres un perro».[1] En 2015, otra caricatura de la misma revista mostraba a otros dos perros hablando: «¿Recuerdas cuando en Internet nadie sabía quién eras?».[2]

En Internet ambas cosas son ciertas. Demostramos que somos quienes decimos ser todo el tiempo, por lo general escribiendo una contraseña que solo nosotros deberíamos conocer. Al mismo tiempo, hay sistemas que permiten que tanto delincuentes como disidentes se comuniquen en secreto sin que los Gobiernos sepan quiénes son (aunque hay muchos casos en los que se enteran de todos modos). También hay sistemas de comunicación anónima, algunos tan simples como crear una cuenta de usuario sin asociarla con un nombre. Y, por último, los piratas informáticos pueden acceder a redes de todo el planeta sin que se sepa quiénes son, aunque también a ellos las empresas de seguridad y los Gobiernos pueden identificarlos a veces.

Si todo esto suena confuso y contradictorio es porque lo es.

LA AUTENTICACIÓN ES CADA VEZ MÁS DIFÍCIL Y EL ROBO DE CREDENCIALES ES CADA VEZ MÁS FÁCIL

En 2016, Rob Joyce, entonces jefe del Grupo de Operaciones de Acceso a Medida de la NSA[3] (TAO, por sus siglas en inglés) y básicamente el principal pirata informático del país, dio una charla pública inusual. En pocas palabras, dijo que las vulnerabilidades del día cero estaban sobrevaloradas y que el robo de credenciales era la forma en la que él se metía en las redes.[4]

Tiene razón. Si bien existen vulnerabilidades en el software, la forma más común de que los piratas informáticos entren en las redes es violando el proceso de autenticación: roban contraseñas, configuran ataques a

intermediarios para conseguir inicios de sesión legítimos o se hacen pasar por usuarios autorizados. El robo de credenciales no requiere encontrar un día cero o una vulnerabilidad sin parches; además, existen menos posibilidades de ser descubierto y le da al atacante mayor flexibilidad con la técnica.

Esto no solo es así para la NSA, sino para todos los atacantes. Fue de esta manera como piratas informáticos chinos accedieron a la Oficina de Administración de Personal de Estados Unidos en 2015.[5] El ataque criminal de 2014 contra Target Corporation comenzó con unas credenciales de inicio de sesión robadas.[6] Desde 2011 hasta 2014, piratas informáticos iraníes robaron las credenciales de inicio de sesión de los líderes políticos y militares de Estados Unidos, Israel y otros países.[7] El *hacktivista* de 2015 que irrumpió en el espacio del fabricante de armas cibernéticas HackingTeam y publicó casi todos los documentos de propiedad de esa compañía usó credenciales robadas.[8] Y en los ataques rusos de 2016 contra el Comité Nacional Demócrata se utilizaron credenciales robadas.[9] Una encuesta encontró que el 80 % de las violaciones de privacidad son el resultado de un abuso o mal uso de las credenciales.[10] Google analizó a los usuarios de Gmail desde mediados de 2016 hasta mediados de 2017 y encontró doce millones de ataques de *phishing* exitosos cada semana.[11]

El robo de credenciales es una línea de ataque muy efectiva porque la autenticación es muy frecuente. Todo lo personal o de tu propiedad está de una forma u otra protegido por contraseñas, por lo que hay muchas oportunidades para descifrarlas. Conseguir que la autenticación sea utilizable y segura es difícil, y en muchos casos imposible, sobre todo porque la mayoría de nuestros sistemas están diseñados de tal manera que, una vez que alguien se autentica, puede hacer casi de todo.

El mecanismo de autenticación más común es mediante nombre de usuario y contraseña; seguro que estás familiarizado con eso. Con tantas contraseñas que recordar, seguro que has hecho cosas que ayudan a hacer este sistema tan inseguro: elegir contraseñas débiles, reutilizar aquellas importantes o escribirlas y dejarlas en lugares públicos.

Los atacantes se aprovechan de estos comportamientos: descifran contraseñas o las roban de tus ordenadores y de servidores, a veces las roban de un sistema y las prueban en otro, adivinan las respuestas a las preguntas secretas para recuperar contraseñas[12] y engañan a los usuarios para que las revelen.

El 19 de marzo de 2016, John Podesta, entonces presidente de la campaña presidencial de Hillary Clinton, recibió un correo electrónico de una unidad

de inteligencia rusa llamada en clave Fancy Bear que fingía ser una alerta de seguridad de Google. Tras un mal asesoramiento por parte del departamento informático, Podesta hizo clic en el enlace y escribió su contraseña en una página de inicio de sesión falsa de Google, lo que le entregó a la inteligencia rusa sus correos electrónicos de una década.[13]

Podesta fue víctima de un ataque de phishing. Es fácil burlarse de él, pero seré comprensivo. Puede ser muy difícil para la víctima, en especial si no tiene conocimientos técnicos, reconocer un mensaje de phishing cuidadosamente diseñado. Si hubiera ignorado el correo electrónico del 19 de marzo, los hackers de Fancy Bear lo habrían intentado una vez más, y luego otra, y solo habrían necesitado tener suerte una de ellas.

El phishing puede ser focalizado o masivo. En un ataque masivo de phishing, descubierto en 2017, los estafadores usaron cuentas pirateadas para enviar correos electrónicos a los contactos de los usuarios con un gusano que se hacía pasar por un archivo de Google Docs que obtenía las credenciales de Google de la víctima cuando se conectaba a Google y luego se reenviaba a todos sus contactos. Google encontró y desactivó el gusano, pero calcula que afectó a un millón de usuarios de Gmail.[14]

Si hay una moraleja en todo esto es que las contraseñas proporcionan una malísima seguridad. Están bien para aplicaciones de baja seguridad, pero nada más.

Hay tres formas básicas de autenticarse: con algo que sabes, con algo que eres y con algo que tienes. Las contraseñas son algo que sabes; te autentican porque en teoría solo tú las conoces.

Un ejemplo de algo que eres es la biometría:[15] huellas dactilares, escáneres faciales o de iris, geometría de manos, etc. Existen muchas formas diferentes. Tanto el iPhone como el Google Pixel, por ejemplo, permiten a los usuarios iniciar sesión en los teléfonos utilizando su huella dactilar o rostro como identificación.

Algo que tienes es un identificador de algún tipo, cosas que llevas contigo para autenticarte.[16] Antes eran objetos físicos con una pantalla que mostraba un número en constante cambio, una tarjeta o un *dongle* que se conectaba a tu ordenador o una clave física que desbloqueaba un sistema. Hoy en día, es más probable que sean aplicaciones o mensajes de texto.

Sin embargo, hay formas de hackear todos estos sistemas. La biometría puede sortearse con fotografías, dedos falsos y cosas por el estilo, y los teléfonos pueden secuestrarse para que el atacante tenga acceso a las

aplicaciones o mensajes de texto. Así que, en general, reemplazar las contraseñas por uno de estos métodos no mejora mucho las cosas.

Usar dos métodos juntos sí mejora la seguridad.[17] Tanto Google como Facebook ofrecen autenticación de dos factores mediante un mensaje de texto en tu teléfono inteligente (esto, por supuesto, tampoco es perfecto, ya que algunas versiones han sido hackeadas).[18] Sprint, T-Mobile, Verizon y AT&T están trabajando juntas para crear un sistema similar.[19] En 2017, Google introdujo su servicio de protección avanzada para usuarios de alto riesgo; entre otras medidas de seguridad, requiere un dispositivo de autenticación que tienes que llevar contigo.[20] Mi red informática en Harvard usa uno de estos sistemas: la combinación de mi contraseña (algo que sé) y una interacción con mi teléfono inteligente (algo que tengo).

Otra opción que estamos empezando a ver es la autenticación diferencial. Facebook puede permitir que te autentiques con una contraseña simple desde tu propio ordenador, pero requerirte otra más compleja si estás usando un ordenador nuevo o extraño. Es posible que tu banco te permita usar tu procedimiento de autenticación normal para transacciones de rutina y que requiera algo más si deseas transferir una gran cantidad o enviar dinero a una cuenta en otro país. También existen investigaciones sobre la autenticación continua basada en tus características biométricas; es decir, si un sistema sabe cómo tiendes a escribir o deslizar tus tarjetas, puede marcar tu cuenta si de repente comienza a comportarse de manera diferente.

La autenticación debe situarse entre la seguridad y la facilidad de uso. Un sistema molesto, sin importar lo seguro que sea, será ignorado por usuarios enfadados. Por ejemplo, escribiremos nuestras contraseñas en una nota adhesiva y las pegaremos en nuestros monitores (suelen aparecer contraseñas en pósits al fondo de fotos y vídeos de la prensa).[21] Una de las mayores ventajas que tiene la biometría sobre las contraseñas es que es más fácil de usar. Una amiga mía solía tener su teléfono desbloqueado porque le molestaba tener que escribir una contraseña. Luego consiguió un Google Pixel con lector de huellas dactilares y, como era tan fácil de usar, comenzó a bloquearlo. Podríamos debatir si estaría más segura con una contraseña compleja, pero no hay discusión posible sobre el hecho de que esté más segura ahora que sin ninguna autenticación.

Ejecutar un sistema de autenticación es difícil. Tanto Google como Facebook ofrecen servicios de autenticación para terceros, y muchos minoristas, blogs y juegos permiten a las personas iniciar sesión con su cuenta de Google o Facebook, lo que en realidad subcontrata la identificación y la

autenticación a esas compañías. Algunos países también lo hacen. El sistema de identificación nacional de Estonia, el que tiene la vulnerabilidad de seguridad mencionada en el capítulo 1, les permite a los ciudadanos y residentes extranjeros acceder a una variedad de servicios gubernamentales, incluida la votación. India ha establecido un sistema de identificación nacional biométrico que será utilizado tanto por organismos gubernamentales como por empresas. Incluso Estados Unidos tienen login.gov, un proveedor centralizado de identidad y autenticación para uso del sector público.

Por un lado, este procedimiento es bueno porque muchos servicios pueden construirse con un único sistema de identidad y autenticación sólido; por otro, crean un único punto de error y, por lo tanto, conllevan un riesgo considerable.

Tu teléfono inteligente se ha convertido en un centro de seguridad centralizado para casi todo.[22] Desde él puedes acceder a todas tus cuentas: correo electrónico, chats, redes sociales, banca y tarjetas de crédito. También es un centro de control para el Internet de las cosas. Si tienes algo de IoT, es probable que lo controles a través de tu teléfono inteligente, desde tu Tesla hasta tu termostato o tus juguetes conectados a Internet. Y todos estos sistemas se basan en la autenticación del teléfono. No tienes que iniciar sesión por separado en tu correo electrónico, Facebook, Tesla o termostato; todas las compañías asumen que, si tienes acceso a tu teléfono, eres tú.

Esto supone un grave error. Los piratas informáticos convencen ahora a los proveedores de telefonía móvil, como Verizon y AT&T, para que transfieran a un dispositivo en su poder el control del número de teléfono de la víctima;[23] una vez que tienen éxito (y es algo que es sorprendentemente fácil de hacer), pueden restablecer todas las cuentas de la víctima que usan su número de teléfono para hacer una copia de seguridad: Google, Twitter, Facebook, Apple… Restablecerán las cuentas bancarias y luego robarán todo su dinero.[24] En el futuro tendremos que autenticarnos para todo —automóviles, aparatos o entorno—, lo que hará que los efectos del compromiso sean considerables.

Otros ataques intentan conseguir una autenticación válida. Un pirata informático monitorizando el ordenador de un usuario puede esperar a que este inicie sesión en un sitio web de banca real y luego manipular lo que el usuario ve en la pantalla y lo que envía al banco para cambiar, por ejemplo, el destino de una transferencia. Esto se denomina *ataque de intermediario* y funciona incluso aunque el banco haya establecido la autenticación de dos factores.[25]

Para defenderse de esto uno puede controlar el sistema en busca de signos de cuentas pirateadas y luego usar la autenticación diferencial. Un ejemplo sería que tu banco se diera cuenta de que acabas de intentar transferir cincuenta mil dólares a una cuenta en Rumanía con la que nunca has hecho transacciones financieras antes y que te llame para verificarla antes de dejar que se realice la transferencia. El emisor de una tarjeta de crédito puede marcar compras de gran valor o cualquier compra de tarjetas regalo donde la tarjeta no esté físicamente presente y retenerlas hasta verificarlas.[26] Algunas aplicaciones bancarias controlan la ubicación del usuario mediante una aplicación de teléfono inteligente y bloquean las compras con tarjeta de crédito realizadas en otro lugar. Para las redes corporativas, hay toda una industria de productos que vigilan la Red en busca de signos de piratería exitosa. Su calidad es variada y suponen otra lucha entre atacante y defensor.

Necesitamos que la autenticación sea fácil de usar y muy segura. Esos son requisitos contradictorios, y vamos a necesitar una forma de pensar inteligente para avanzar en este punto. Aun así, la autenticación será incluso menos conveniente de lo que es ahora, y no hay forma de evitarlo.

Esto siempre me recuerda a las personas de la generación de mis abuelos, que nunca se acostumbraron a guardar las llaves. Tenían la costumbre de dejar sus puertas siempre abiertas y les molestaba tener que cerrar con llave: debían acordarse, siempre tenían que llevar una llave consigo, sus amigos no podían entrar sin una, etc. Es un inconveniente al que he estado acostumbrado toda mi vida. Claro, me he quedado encerrado fuera de casa y he tenido que llamar a mi esposa para que me ayudara o pagar a algún cerrajero alguna vez. Pero para mí solo se trata de una pequeña molestia a cambio de una casa más resistente a los ladrones. Pasa lo mismo con los cinturones de seguridad; cuando era pequeño nadie los llevaba, pero hoy en día los niños no dejarían que las personas condujeran a menos que lo lleven abrochado. Del mismo modo, me he adaptado a los sistemas de autenticación de dos factores: un pequeño inconveniente para que mi cuenta sea más segura frente a los piratas informáticos.

La autenticación es fundamental para Internet+. Casi todas las cosas informatizadas usarán algún sistema de autenticación para saber con quién deben hablar, a quién escuchar y quién puede controlarlas. Esto se aplica a grandes cosas, como tu vehículo y las plantas de energía nuclear, y también a otras más pequeñas, como juguetes y bombillas inteligentes. Nos autenticaremos delante de las cosas todo el tiempo y ellas también lo harán.

Gran parte de Internet+ se basará en la identificación y en la autenticación, pero los sistemas fiables y escalables para hacerlo aún no existen. Tu termostato querrá hablar con tu horno, tus electrodomésticos querrán hablar con tu contador eléctrico y tus juguetes querrán hablar entre ellos.

Las actualizaciones necesitan autenticarse para evitar que los atacantes te engañen para que instales alguna que sea maliciosa; fue una de las técnicas que usó Stuxnet.[27] Durante años, sin embargo, los piratas informáticos han estado utilizando autorizaciones de firma válidas para crear firmas de autenticación válidas para las actualizaciones malas.[28] Muchas de las vulnerabilidades de la cadena de suministro de las que hablaremos en el capítulo 5 son el resultado de una autenticación defectuosa.

Algunas de estas comunicaciones serán críticas. Los coches se comunicarán entre ellos, tanto lo que vean desde sus sensores como sus intenciones; los dispositivos médicos lo harán entre sí y con los médicos y, en función de ello, cambiarán su comportamiento; la compañía eléctrica local, con los principales electrodomésticos de la comunidad, y también los diferentes sistemas de construcción estarán comunicados. Como aprendimos en el capítulo 2, cada dispositivo deberá recibir parches de seguridad autenticados. Todo esto tendrá lugar de forma automática y sucederá constantemente, millones de veces al día.

No sabemos cómo afrontar esto. El protocolo que utilizamos para conectar dispositivos cercanos es *bluetooth*, y solo funciona porque estamos involucrados en el proceso durante la configuración. Cuando conectamos nuestros teléfonos con nuestro coche, por ejemplo, nos estamos autenticando unos a otros y permitimos que los dispositivos se comuniquen después sin nuestra participación. Pero es algo factible si solo existen unos pocos dispositivos que necesiten emparejarse. Cuando tengamos miles de ellos tratando de comunicarse entre sí, será imposible que lo hagamos de forma manual. Y aunque el modelo hup-and-spoke, basado en concentrar las autenticaciones por medio de las autoridades centrales (como nuestros smartphones), solucionará algo de esto, no lo solucionará del todo.

Los ataques tendrán graves consecuencias. Si puedo hacerme pasar por ti en tus dispositivos, puedo aprovecharme de ti. Este es el robo de identidad del futuro, y da miedo. Si puedo alimentar tus dispositivos con información defectuosa, puedo manipularlos de manera dañina. Si puedo engañar a tus dispositivos para que piensen que soy más fiable que tú, puedo dar

instrucciones en tu nombre. No entendemos del todo las consecuencias de estos ataques porque tampoco entendemos bien el alcance de los sistemas.

Esto nos lleva a la identificación. Nos identificamos cuando configuramos cuentas en persona o en Internet. Lo sólida que sea la identificación depende de la cuenta. Con un banco, es bastante fiable por tratarse de una interacción cara a cara en una sucursal, mientras que con una compra con tarjeta de crédito es más débil y se basa en que una persona conozca un montón de información personal. A veces la identificación está vinculada con un número de teléfono, una dirección, un carné de identidad o un permiso de conducir. Facebook tiene una *política de nombres reales*: se supone que las personas usan sus verdaderos nombres, pero no hay ninguna verificación a menos que exista una disputa de algún tipo.[29] Google solicita un número de teléfono para configurar una cuenta de Gmail, aunque las personas pueden usar un teléfono de prepago anónimo.[30] Otras veces la identificación no se basa en nada. Mi cuenta de Reddit no es más que un nombre de usuario convertido en pseudónimo, ya que la única identificación es para la página y para todas las publicaciones que he hecho con ese nombre.

Atar algo a tu identidad significa que tienes una manera fiable de demostrar que eres tú y que nadie más lo es. Incluye autenticación, pero es algo más fuerte. Puedes autenticar una cuenta bancaria anónima, lo que demuestra que eres la misma persona que depositó el dinero la semana pasada. La identificación de esa cuenta prueba que el dinero te pertenece, es decir, que está a tu nombre.

La identificación nunca es infalible. Para obtener un pasaporte tengo que ir en persona a solicitarlo, así que, para hacerme pasar por otra persona, tendría que ser capaz de falsificar los documentos de filiación o identidad que se me exigen (aquellos que identifican a las personas para que puedan obtener un nuevo documento de identificación). Difícil, pero no imposible. Hay gente que ha obtenido permisos de conducir reales con nombres falsos utilizando documentos falsificados. Es más difícil cuando el Gobierno sigue la pista de sus ciudadanos desde su nacimiento, aunque eso tiene otros problemas asociados.

La suplantación siempre será más fácil si se hace de forma remota. Una vez más, seguridad frente a conveniencia. Las grandes empresas que nos reclaman siempre van a preferir la conveniencia. Nosotros también. Al final, ambos necesitaremos un empujón hacia la seguridad.

LA ATRIBUCIÓN CADA VEZ ES MÁS DIFÍCIL Y MÁS FÁCIL; DEPENDE

La atribución es la identificación de alguien que no quiere que lo identifiquen. Pero, si bien esa persona quiere permanecer en el anonimato, las autoridades querrán identificarla. Tal vez esté cometiendo un fraude o quizá esté tratando de obtener acceso no autorizado a una central nuclear. Podría estar publicando en algunos países material contra el Gobierno o intentando descargar pornografía. En todos estos casos, los agentes de la ley querrán atribuir las acciones a alguna persona o a un grupo identificable.

La mayor parte del tiempo la atribución es fácil. Si la persona está usando una cuenta asociada con su número de tarjeta de crédito, su nombre real o su número de teléfono, solo hay que conseguir esa información de cualquier proveedor de servicios que la tenga. Es posible que haya obstáculos legales (podría exigirse la obtención de una orden judicial, o puede haber problemas jurisdiccionales si la información está en otro país), pero no existen obstáculos técnicos.

A veces la atribución es difícil, aunque sigue siendo posible. Incluso las personas que se esfuerzan por ocultar su identidad descubren que se equivocan.

Ross Ulbricht era Dread Pirate Roberts, el hombre estadounidense detrás del sitio de comercio electrónico Silk Road, de bienes y servicios ilegales. Lo encontró un tenaz agente del FBI uniendo el descubrimiento de un correo de hacía años en un chat, una antigua dirección de correo electrónico y una entrevista casual con agentes del FBI que investigaban otra cosa.[31]

Se ha identificado y detenido a pedófilos por detalles que se apreciaban en el fondo de fotografías: un camping en Minnesota, la marca de una sudadera o un paquete de patatas fritas.[32] También identificaron y detuvieron a un bielorruso que manejaba la enorme red de robots Andrómeda porque reutilizó sin querer un número de cuenta de mensajería instantánea asociado con su nombre real,[33] o al hacker de Texas Higinio O. Ochoa III porque los metadatos de la ubicación de una fotografía condujeron a los investigadores hasta su novia.[34]

Este tipo de atribución puede ser caro y llevar mucho tiempo. Si alguien puede tener presencia en Internet y esconderse de la policía, depende tanto de la habilidad y el cuidado de esa persona como de la pericia y los fondos de la policía que esté tratando de desenmascararla. La mayoría de las veces no vale la pena atribuir acciones individuales en Internet.

Las cosas son muy diferentes cuando se trata de organizaciones de inteligencia nacionales, como la NSA, que puede vigilar amplias franjas de Internet. Para ellos, la atribución es mucho más fácil.

En 2012, el entonces secretario de Defensa de Estados Unidos Leon Panetta dijo públicamente que Estados Unidos (al parecer la NSA) había logrado avances significativos en la identificación de los orígenes de los ataques cibernéticos.[35] Otros funcionarios del Gobierno de Estados Unidos han dicho en privado que han resuelto el llamado problema de la atribución. [36] No sabemos cuánto de esto es verdad, aunque creo que estas afirmaciones son bastante ciertas.

En la charla de 2016 con la que comenzaba este capítulo, Rob Joyce, de la NSA, dijo lo siguiente:

> Es sorprendente la cantidad de abogados que tienen el DHS, el FBI y la NSA, por lo que, si el Gobierno dice que también tenemos una atribución positiva, debemos creerlo. La atribución es realmente difícil, así que cuando el Gobierno lo dice, estamos utilizando todas las fuentes y los métodos que tenemos para ayudar a informar sobre ello. [Pero] debido a que estas amenazas persistentes avanzadas no desaparecen… no podemos poner toda esa información en primer plano y ser totalmente transparentes sobre todo lo que sabemos y cómo lo sabemos. [37]

Este es un tipo de atribución en el ámbito nacional. Y, mientras que la NSA a veces puede identificar a personas individuales (Estados Unidos acusó a cinco chinos de piratear corporaciones estadounidenses[38] en 2014 y a trece rusos por interferir en las elecciones estadounidenses de 2016),[39] es más fácil atribuir ataques a una nación en particular.

Básicamente, la NSA ha eliminado el anonimato gracias a la vigilancia masiva. Si puedes verlo todo, puedes unir pistas dispares y descubrir qué está pasando y quién es quién. Tal vez incluso puedas hacerlo de forma automática, que es lo que países como China y Rusia están tratando de hacer con su amplia vigilancia de Internet.

No asumamos que la falta de atribución pública signifique que esta no existe. Si tras la atribución no hay una respuesta efectiva, un país se verá débil, por lo que tiene sentido que, a menudo, algunas naciones no atribuyan públicamente un ataque cibernético cuando no son capaces de responder a él. [40]

Además, gran parte de la información que recopila la NSA está clasificada. Y aunque podría estar bien divulgarla, los detalles a menudo revelan cómo se ha conseguido; es decir, las fuentes y métodos a los que se refiere Joyce, que también son secretos. Esto significa que, con frecuencia, el Gobierno de Estados Unidos no puede explicar por qué le atribuye un ataque a un país o a un grupo en particular, lo que significa que no hay manera de verificar por otro lado tal atribución. Esto es negativo si eres alguien que tiende a desconfiar del Gobierno. Y mientras que es obvio que la NSA necesita mantener sus fuentes y métodos en secreto, los funcionarios del Gobierno deberán exponerlos si esperan que la sociedad en general crea en sus argumentos de atribución y apoyen cualquier acción de represalia que tomen.

Los puntos principales son los siguientes: 1) la atribución puede ser difícil, en especial para los países que no realizan una vigilancia amplia de Internet ni tienen experiencia forense dentro de sus propias organizaciones; 2) la atribución lleva tiempo, pueden pasar semanas o meses antes de que el país víctima sepa quién lo atacó; 3) la naturaleza virtual de los ataques y la facilidad para ocultar sus orígenes significa que el país atacante siempre puede negarlo; 4) la atribución puede basarse en información clasificada que puede hacer que sea difícil refutar esas negaciones, y 5) los actores de Estados no nacionales tienen muchas de las mismas capacidades que los países, lo que dificulta aún más determinar si el liderazgo del país es en realidad responsable.[41]

El hackeo de Sony Pictures realizado por los norcoreanos en 2014, quienes publicaron tanto información de la compañía como películas inéditas, es un buen ejemplo del problema de la atribución. En los días posteriores al ataque hubo un debate legítimo sobre si este fue perpetrado por un Estado nación con un presupuesto militar de 20.000 millones de dólares o por un par de tipos en un sótano en cualquier sitio. (Yo estaba en el lado equivocado de este debate: apostaba por el par de tipos.)[42] Pasaron tres semanas antes de que Estados Unidos atribuyera definitivamente los ataques a Corea del Norte, aunque, debido a que gran parte de las pruebas de la atribución eran secretas, muchos expertos en seguridad informática no se lo creyeron. No creí al Gobierno hasta que *The New York Times* informó sobre algunas de las pruebas de inteligencia de la NSA.[43]

Hay una brecha de atribución en este momento entre países que son buenos en eso y países que no. A países como China les preocupa que Estados Unidos pueda atribuirles ataques públicamente, pero que no puedan nombrar

y avergonzar a otros países de la misma manera. Otros más pequeños, como Estonia y Georgia, tienen muchas menos esperanzas de descubrir quién los ataca en el ciberespacio. No es imposible: las compañías de antivirus suelen atribuir ataques, pero es difícil y lleva incluso más tiempo. Y nadie más está al nivel de la NSA.

A nivel estatal, esto resultará en una lucha entre la detección y la evasión. Creo que evadir la detección será más fácil en el futuro, al menos cuando se trata de los atacantes más capaces. En este momento Rusia no hace demasiado por ocultar sus huellas porque no existen muchas represalias y deja de preocuparse si la amonestan.[44] A medida que las tecnologías de atribución se vuelvan más sofisticadas, y si comenzamos a tomar represalias, los países harán un esfuerzo mayor por ocultarse o por culpar falsamente a un tercero.

Un tipo diferente de enfrentamiento tendrá lugar de manera individual. La gente continuará cometiendo errores y la policía mejorará en la atribución de ataques, pero siempre habrá personas que sean hábiles, afortunadas o que no tengan la suficiente importancia como para permanecer en el anonimato.

04

TODO EL MUNDO FAVORECE LA INSEGURIDAD

LOS FALLOS EN LA TECNOLOGÍA no son la única razón por la que Internet es tan inseguro. Otra razón importante, tal vez incluso la principal, es que los más poderosos en Internet —Gobiernos y empresas— han manipulado la Red para que sirva a sus propios intereses.

Todos quieren que tengas seguridad, pero no que proceda de ellos. Google está dispuesto a proporcionarte seguridad siempre que pueda vigilarte y utilizar esa información para vender anuncios. Facebook te ofrece un trato similar: una red social segura, pero que puede controlar todo lo que haces con fines de marketing. El FBI quiere que tengas seguridad siempre que pueda romperla si así lo desea.[1] La NSA es exactamente igual, lo mismo que sus equivalentes en el Reino Unido, Francia, Alemania, China, Israel y otros lugares.

Las razones difieren (y nunca lo admitirán con tanta claridad), pero básicamente la inseguridad está al servicio de las empresas y los Gobiernos. Ambos se benefician de las lagunas en la seguridad y trabajan para mantenerlas. Las empresas quieren inseguridad por razones lucrativas y los Gobiernos por razones de aplicación de la ley, control social, espionaje internacional y ataque cibernético. La dinámica de todo esto es complicada, por lo que iremos paso a paso.

EL CAPITALISMO DE VIGILANCIA SIGUE IMPULSANDO INTERNET

Las empresas quieren tus datos; las páginas web que visitas intentan descubrir quién eres y qué quieres, y están vendiendo esa información; las aplicaciones de tu teléfono inteligente están recopilando y vendiendo tus datos, y los sitios de redes sociales que frecuentas venden tus datos o el acceso a ti en función

de estos. La profesora de la Escuela de Negocios de Harvard Shoshana Zuboff llama a esto *capitalismo de vigilancia*[2] y es el modelo de negocios de Internet: las empresas construyen sistemas que espían a las personas a cambio de servicios.

Esta vigilancia es fácil porque los ordenadores lo hacen de manera natural. Los datos son un subproducto de los procesos informáticos. Todo lo que hacemos que involucra un ordenador crea un registro de transacciones; esto incluye navegar por Internet, usar o tan solo cargar un teléfono móvil, hacer una compra en línea o con una tarjeta de crédito, caminar por un sensor informatizado o decir algo en la misma habitación que la Alexa de Amazon. Los datos también son un subproducto de cualquier tipo de socialización usando ordenadores: las llamadas telefónicas, los correos electrónicos, los mensajes de texto y las conversaciones de Facebook crean registros de transacciones. Como he indicado con anterioridad, todos estamos dejando un rastro de migas de pan digitales a medida que avanzamos en nuestras vidas.

Nuestros datos solían desecharse porque su valor era muy marginal y su uso difícil, pero esos tiempos han terminado. Hoy en día, el almacenamiento de datos es tan barato que todos pueden guardarse. Esta es la materia prima de los macrodatos (*big data*). Se trata de datos de vigilancia recopilados y utilizados por las empresas, sobre todo para defender el modelo de publicidad que respalda gran parte de Internet.

Si observas las listas de las compañías más valiosas del mundo en la última década, encontrarás las que participan en el capitalismo de vigilancia: Alphabet (la empresa matriz de Google), Facebook, Amazon y Microsoft. Apple es la excepción: solo gana dinero vendiendo hardware, motivo por el que sus precios son más altos que los de la competencia.

El modelo publicitario de Internet es cada vez más personal. Las empresas tratan de averiguar tus emociones,[3] determinar a qué le prestas atención y cómo reaccionas[4] y saber a qué imágenes respondes y exactamente cómo adularte;[5] hacen todo esto para enviarte publicidad de manera más precisa y efectiva, y así venderte cosas.

Nadie sabe cuántos corredores de datos y compañías de seguimiento operan en Estados Unidos; he leído unas estimaciones de 2.500 a 4.000.[6] Estas corporaciones saben una gran cantidad de cosas acerca de nosotros gracias a los dispositivos que usamos y llevamos. Nuestros teléfonos móviles revelan nuestra ubicación en todo momento: dónde vivimos, dónde trabajamos, con quién pasamos el tiempo; saben cuándo nos despertamos y cuándo nos vamos a dormir (porque revisarlos suele ser lo primero y lo último

que hacemos cada día) y, como todos tenemos un teléfono móvil, también saben con quién nos vamos a la cama.

Considera por un momento quién más sabe dónde está tu teléfono inteligente y, por lo tanto, dónde te encuentras. Esa lista incluiría cualquier otra aplicación a la que le hayas dado permiso para rastrear tu ubicación (y algunas que lo hacen por otros medios).[7] Las obvias son Google Maps y Apple Maps, aunque también hay otras menos evidentes. En 2013, unos investigadores descubrieron que las aplicaciones como Angry Birds, Pandora Internet Radio y Brightest Flashlight (sí, una aplicación de linterna) también localizaban la ubicación de sus usuarios.[8]

Los teléfonos inteligentes ahora contienen muchos sensores diferentes. Cualquier red wifi a la que te conectes puede determinar tu ubicación, o incluso tu teléfono cuando trata de conectarse a ellas mientras caminas.[9] El bluetooth de tu móvil puede notificar a los ordenadores próximos que estás cerca. La empresa Alphonso ofrece a las aplicaciones la capacidad de usar el micrófono del teléfono para recopilar datos sobre lo que la gente está viendo en televisión.[10] Facebook tiene una patente sobre el uso de lecturas de acelerómetro y giroscopio de múltiples teléfonos para detectar cuándo dos personas están frente a frente o caminan juntas.[11] Y suma y sigue.

Hay otras formas de determinar tu ubicación. ¿Has pagado con tu tarjeta de crédito en una tienda?, ¿has usado un cajero automático?, tal vez pasaste por una de las miles de cámaras de seguridad en una ciudad y, aunque la cámara probablemente no te identificó (pronto el reconocimiento facial automático se volverá lo bastante común como para hacerlo), un escáner automático de matrículas registró tu vehículo.[12]

Las empresas de vigilancia saben mucho de nosotros. Quizá Google sea el mejor ejemplo.[13] La búsqueda en Internet es muy personal: nunca les mentimos a nuestros motores de búsqueda.[14] Nuestros intereses y curiosidades, esperanzas, temores, deseos y tendencias sexuales son recopilados y guardados por las compañías que buscan en Internet en nuestro nombre.

Para que quede claro: cuando digo «Google sabe» o «Facebook sabe», no estoy dando a entender que las empresas sean sabias o incluso conscientes. Más bien me refiero a dos cosas muy específicas: una, que los datos existentes en los ordenadores de Google le permitirían a una persona que tiene acceso a ellos, ya sea autorizada o no, conocer los hechos si así lo desea, y dos, que los algoritmos automáticos de Google pueden usar esta

información para hacer inferencias sobre nosotros y realizar tareas automatizadas basadas en ellas.

En el futuro nuestros dispositivos podrán reconstruir un modelo sorprendentemente profundo de quiénes somos, qué pensamos, adónde vamos y qué hacemos. Los frigoríficos controlarán nuestro consumo de alimentos y, por extensión, nuestra salud; nuestros coches sabrán cuándo y con qué frecuencia violamos las leyes de circulación, y podrían informar a la policía o a nuestras compañías de seguros; las pulseras de actividad deportiva intentarán descubrir nuestros estados de ánimo o nuestras camas sabrán lo bien que hemos dormido. Todos los automóviles Toyota nuevos controlan la velocidad, la dirección, la aceleración y el frenado, incluso aunque el conductor tenga las manos en el volante.[15]

Las tentaciones gemelas del capitalismo de vigilancia son *gratuitas* y *convenientes*. Esto ha configurado el Internet comercial durante más de dos décadas, y pronto lo hará con muchas más cosas. Y requiere de inseguridad para operar al máximo rendimiento. Mientras las empresas tengan la libertad de recopilar la mayor cantidad de información posible sobre nosotros, no protegerán de forma adecuada nuestros sistemas. Siempre que compren, vendan, intercambien y almacenen esos datos, existirá el riesgo de que nos roben; y mientras los usen, corremos el riesgo de que sea en nuestra contra.

EL CONTROL CORPORATIVO DE CLIENTES Y USUARIOS ES LO SIGUIENTE

Los ordenadores no solo permiten que nos vigilen de una manera nunca antes vista, sino también que nos controlen. Es un nuevo modelo de negocio: nos obligan a pagar funciones individuales, usar accesorios específicos o suscribirnos a productos y servicios que ya hayamos adquirido antes. Este tipo de control se ampara en la inseguridad de Internet.

Si eres un agricultor que acaba de comprar un tractor John Deere, tal vez pienses que ya es tuyo. Quizá fuera así en el pasado, pero las cosas son diferentes hoy en día. Debido a que los tractores contienen software, porque en esencia son solo ordenadores con un motor, ruedas y una cosechadora acoplada, John Deere ha podido pasar de un modelo de negocio de propiedad a uno de licencia. En 2015, John Deere le dijo a la Oficina de Derecho de Autor de Estados Unidos que los agricultores reciben «una licencia implícita durante la vida útil del vehículo para operar el vehículo»,[16] y esa licencia viene con todo tipo de reglas y advertencias: por ejemplo, los agricultores no

tienen ahora derecho a reparar o modificar sus tractores; en su lugar, tienen que usar equipos autorizados de diagnóstico, piezas e instalaciones de reparación sobre los que John Deere tiene el monopolio.

Apple mantiene un control estricto sobre qué aplicaciones están disponibles en su tienda. Antes de vender o regalar una aplicación a los clientes de iPhone, Apple tiene que aprobarla, y la compañía tiene unas reglas muy estrictas sobre lo que permite y lo que no: nada de pornografía, por supuesto, ni juegos sobre trabajo infantil o tráfico de personas, pero tampoco aplicaciones políticas. Esta última regla supuso que Apple censurara las aplicaciones que rastreaban ataques de drones de Estados Unidos[17] y las que incluían «contenido que ridiculiza a las figuras públicas».[18] Tales restricciones colocaban a Apple en una situación que favorecía la aplicación de las exigencias de censura del Gobierno. Y así ha sido: en 2017, Apple eliminó las aplicaciones de seguridad de su tienda en China.[19]

Apple es un ejemplo extremo, pero no es la única compañía que censura tu Internet. Facebook censura a menudo publicaciones, imágenes y sitios web completos, YouTube censura vídeos y Google, los resultados de búsqueda, además de prohibir una aplicación que hace clic al azar en los anuncios de su navegador Chrome porque interfiere con su modelo de negocio de publicidad.[20]

Por lo general, no nos supondría un problema que una empresa tomara decisiones sobre qué productos elige tener. Si Walmart no vende CD de música con etiquetas de advertencia para los padres, podemos comprarlo en cualquier otro lugar. Pero muchas empresas de Internet pueden ser muy poderosas, más que las tiendas físicas, incluso por encima de cadenas tan grandes como Walmart, porque se benefician de lo que se llama el efecto red; es decir, cuantas más personas consumen en ellas, más útiles se vuelven. Un teléfono es inútil y dos son medianamente útiles, pero una red completa de teléfonos es muy útil. Lo mismo ocurre con las máquinas de fax, el correo electrónico, la web, los mensajes de texto, Snapchat, Facebook, Instagram, PayPal y todo lo demás. Cuantos más consumidores tengan, más útiles son. Y cuanto más poderosas sean las compañías que las manejan, más control pueden ejercer sobre ti.

A menos que sepas cómo liberar tu teléfono para eliminar sus restricciones, descargar aplicaciones y vivir con un dispositivo sin garantía que no pueda actualizarse sin requerir esfuerzo, la tienda de iTunes es el único lugar al que puedes acceder para las aplicaciones de iPhone. Entonces,

si Apple decide no incluir una aplicación, no hay forma de que los clientes corrientes la obtengan.

En la mayoría de los casos el control equivale a beneficio. Facebook controla cómo las personas llegan hasta las noticias mientras les resta poder —e ingresos por publicidad— a los periódicos y revistas tradicionales. Amazon controla cómo las personas compran sus cosas y les quita el poder a los minoristas tradicionales. Google controla cómo las personas encuentran la información que necesitan, lo que disminuye el poder de todos los sistemas de información más tradicionales. La batalla por la neutralidad de la Red tiene que ver con los proveedores de telecomunicaciones, que desean controlar tu experiencia en Internet.

En obras anteriores he descrito la situación en Internet como feudal: renunciamos al control de nuestros datos y capacidades a cambio de servicios. Decía lo siguiente:

> Algunos le han prometido lealtad a Google: tienen cuentas de Gmail, usan Google Calendar y Google Docs, y tienen teléfonos Android, probablemente Pixel. Otros le han jurado lealtad a Apple: tienen ordenadores portátiles Macintosh, iPhones y iPad, y dejan que iCloud se sincronice automáticamente y haga una copia de seguridad de todo. Algunos dejan que Microsoft lo haga todo. O compran su música y sus libros electrónicos de Amazon, que mantiene registros de lo que poseen y permite la descarga a un Kindle, ordenador o teléfono. Otros han abandonado el correo electrónico por completo… y lo han cambiado por Facebook.[21]

Estas compañías son como señores feudales que nos protegen de amenazas externas, pero a la vez también tienen un sorprendente y completo control sobre lo que se nos permite ver y hacer.

Las empresas están viendo a Internet+ de la misma manera. Philips quiere que su controlador sea el eje central de sus bombillas y otros dispositivos electrónicos, Amazon quiere que Alexa sea el centro de toda tu casa inteligente, tanto Apple como Google quieren que sus teléfonos sean el dispositivo único a través del cual controles todos sus dispositivos IoT. Todos quieren ser centrales, esenciales y tener el control de tu mundo.

Y las empresas regalarán servicios para conseguirlo. De la misma manera que Google y Facebook ofrecen servicios a cambio de la posibilidad de espiar a sus usuarios, las empresas harán lo mismo con el IoT: ofrecerán material del IoT gratuito a cambio de los datos que reciben controlando a las personas que

lo utilizan. Las compañías de vehículos autónomos pueden regalar viajes a cambio de la posibilidad de mostrar anuncios a los pasajeros, conseguir sus contactos, dirigirlos a alguna parte o hacer una parada intermedia en ciertos restaurantes y tiendas.[22]

La batalla por el control de clientes y usuarios se va a calentar en los próximos años. Y, dado que las posiciones monopolísticas de compañías como Amazon, Google, Facebook y Comcast les permiten ejercer un control significativo sobre sus usuarios, las compañías más pequeñas, obviamente menos basadas en la tecnología, como John Deere, están intentando hacer lo mismo.

Todo este poder corporativo se basa en abusar de la DMCA (la misma ley de la que hablábamos en el capítulo 2), que obstaculiza el parcheo de las vulnerabilidades del software. La DMCA fue diseñada por la industria del entretenimiento para proteger los derechos de autor; es una ley perniciosa que ha proporcionado a las corporaciones la capacidad de hacer cumplir sus preferencias comerciales dentro del Estado de derecho. Debido a que el software está sujeto a derechos de autor, protegerlo con un sistema de administración de derechos digitales (DRM, por sus siglas en inglés) contra la copia se acoge a la DMCA. Esta ley hace que sea un delito analizar y eliminar la protección contra copias y, por lo tanto, analizar y modificar el software. John Deere aplica sus prohibiciones de que los agricultores se encarguen del mantenimiento de sus propios tractores protegiendo los ordenadores incorporados en ellos.

Las cafeteras Keurig están diseñadas para usar las cápsulas K-cup para preparar cafés individuales. Debido a que las máquinas usan software para verificar el código impreso en las cápsulas, Keurig puede imponer su exclusividad, por lo que solo las compañías que pagan a la empresa pueden producir cápsulas para sus cafeteras.[23] Las impresoras HP ya no te permiten utilizar cartuchos de tinta no autorizados.[24] Es posible que mañana una empresa te exija que utilices solo papel autorizado (o que se niegue a imprimir palabras con derechos de autor que no hayas pagado). Del mismo modo, el lavavajillas de mañana podría imponer las marcas de detergente que usa.

A medida que Internet+ lo convierte todo en ordenadores, los softwares estarán amparados por la DMCA. Este mismo truco legal se emplea para ligar los periféricos a los productos, obligar a los consumidores a comprar solo componentes compatibles autorizados o contratar servicios de reparación en distribuidores autorizados. Esto afecta a los teléfonos inteligentes, los

termostatos, las bombillas inteligentes, los automóviles y los implantes médicos. Y aunque algunas compañías se hayan excedido en sus reclamaciones de DMCA y hayan perdido en los tribunales,[25] todavía es una táctica común.

Con frecuencia, el control del usuario va de la mano con la vigilancia. Con el fin de garantizar el cumplimiento de las restricciones que les imponen a sus clientes y usuarios, las empresas supervisan a menudo lo que estos están haciendo. Luego les niegan a los clientes el acceso a esos datos. Por ello, los clientes se están rebelando.

Cada vez más las personas tratan de piratear sus propios dispositivos médicos. Hugo Campos es una de ellas. Durante años ha tenido un desfibrilador cardioversor implantado que controla su afección cardíaca, pero también recopila continuamente datos sobre su corazón. Imagínate algo así como un Fitbit con capacidades de electroshock. Pero, a diferencia de un Fitbit, el implante de Campos está patentado y él no puede acceder a los datos, por lo que ha recurrido a demandar al fabricante —hasta ahora sin éxito —. Ninguna de las compañías que fabrican dispositivos implantables (Medtronic, Boston Scientific, St. Jude Medical y Biotronik) permitirá a los pacientes acceder a sus propios datos, y nadie puede hacer nada al respecto. Los datos son propiedad de las empresas.[26]

De manera similar, algunas personas han pirateado sus Toyota Prius desde 2004 para mejorar la eficiencia del combustible,[27] deshabilitar las advertencias molestas, obtener mejor información de diagnóstico del motor, modificar su rendimiento y acceder a las opciones disponibles en las versiones europea y japonesa del automóvil, pero no en la versión de Estados Unidos. Estos trucos pueden anular la garantía, pero los fabricantes de automóviles no pueden pararlos. Hay pirateos y códigos para muchos otros modelos de vehículos.[28]

No hay mucha diferencia con respecto a los datos de la caja negra del vehículo;[29] la policía y las compañías de seguros utilizan los datos después del accidente,[30] pero los usuarios no tienen acceso a ellos. (Una ley de California que permitía que las personas accedieran a los datos de su vehículo se estancó debido a la oposición de los fabricantes.)[31] Por su parte, los propietarios de tractores John Deere han recurrido a la compra de firmware pirata de Ucrania para reparar ellos mismos sus tractores.[32]

Esto no es una cuestión de blanco o negro. No queremos que las personas tengan una capacidad sin restricciones para hackear sus propios dispositivos de consumo. Por ejemplo, los termostatos tienen amplios límites de control; si

alguien cambia el software para mantener la temperatura de manera más precisa, puede dañar el sistema de calefacción al encenderlo y apagarlo con demasiada frecuencia. Del mismo modo, ese software de tractor pirata de Ucrania podría eliminar, ya sea accidentalmente o a propósito, una parte del software que protege la transmisión, lo que haría que fallara más a menudo. Si John Deere es el responsable de las reparaciones de la transmisión, eso supone un problema.

Asimismo, no queremos que las personas pirateen sus coches, de manera que infrinjan las leyes de control de emisiones, o sus dispositivos médicos, de modo que eludan las restricciones legales que rodean el uso de esos aparatos. Por ejemplo, hay personas que piratean sus bombas de insulina para crear un páncreas artificial: un dispositivo que mida sus niveles de azúcar en la sangre y administre las dosis adecuadas de insulina de forma continua y automática. [33] ¿Queremos darles la posibilidad de hacer eso o queremos asegurarnos de que solo los fabricantes regulados produzcan y vendan esos dispositivos? No estoy muy seguro.

Cuanto más se extienda Internet+ a diferentes espacios de nuestras vidas, este tipo de conflicto se desarrollará en todas partes. Las personas querrán acceder a los datos de sus máquinas de hacer ejercicio, de sus electrodomésticos, de los sensores domésticos y de sus vehículos, y querrán la información en sus propios términos, de forma que puedan usarla para los fines que deseen, como la posibilidad de modificar los dispositivos para añadir funcionalidades. Los fabricantes y los Gobiernos tratarán de evitarlo; a veces será con fines lucrativos o por razones anticompetitivas, otras por motivos legales y algunas veces será solo porque los proveedores no se molestaron en hacer accesibles los datos o los controles.

Todo esto reduce la seguridad. Para que las empresas nos controlen a su antojo, construirán sistemas que permitan el control remoto. Más importante aún, construirán sistemas que asuman que el cliente es el atacante, alguien a quien deben contener. Este es un requisito de diseño que va contra la buena seguridad, ya que les proporciona a los atacantes externos una vía para obtener acceso. Al mismo tiempo, los piratas informáticos pueden incluir inseguridades para hacerse con el control a través de las modificaciones que hagan los clientes por la puerta de atrás.

LOS GOBIERNOS TAMBIÉN UTILIZAN INTERNET PARA LA VIGILANCIA Y EL CONTROL

Los Gobiernos quieren vigilarnos y controlarnos para sus propios fines, y para hacerlo usan los mismos sistemas inseguros que las empresas nos han dado.

En 2017, el centro de investigación Citizen Lab de la Universidad de Toronto informó sobre lo que la vigilancia del Gobierno mexicano consideraba amenazas políticas. Ese país adquirió software de vigilancia (*spyware* o software espía) del fabricante de ciberarmas NSO Group y lo utilizó para espiar a periodistas,[34] disidentes, rivales políticos,[35] investigadores internacionales,[36] abogados,[37] grupos anticorrupción[38] y personas que apoyaban un impuesto sobre los refrescos.[39]

Muchos otros países usan spyware de Internet para vigilar a sus residentes. Se sabe que los productos de FinFisher, otra compañía comercial de software espía, se utilizaron en 2015 en Bosnia, Egipto, Indonesia, Jordania, Kazajistán, Líbano, Malasia, Mongolia, Marruecos, Nigeria, Omán, Paraguay, Arabia Saudí, Serbia, Eslovenia, Sudáfrica, Turquía y Venezuela.[40] Este software estaba destinado a disidentes, activistas, periodistas y otras personas que los Gobiernos de estos países querían arrestar, intimidar o simplemente controlar.

La vigilancia gubernamental para el control político y social es normal en Internet hoy. Las mismas tecnologías que nos dieron el capitalismo de vigilancia también permiten a los Gobiernos llevar a cabo su propia vigilancia. El grado en que esto ha estado ocurriendo solo ha salido a la luz en los últimos años, y no muestra signos de desaceleración. De hecho, es probable que Internet+ traiga consigo más vigilancia gubernamental, parte de ella para bien, pero mucha de ella para mal.

La vigilancia moderna del Gobierno va a caballo con la corporativa ya existente. No es que la NSA se haya despertado una mañana y haya dicho «Vamos a espiarlos a todos». En vez de eso dijo: «Las corporaciones de Estados Unidos están espiando a todo el mundo. Hagámoslo también nosotros». Y lo hizo, a través de sobornos, coerción, amenazas, imposiciones legales y robo directo:[41] recopilación de datos de ubicación de teléfonos móviles, de las *cookies* de Internet, de correos electrónicos y mensajes de texto, de los inicios de sesión, etc.[42] Otros países actúan de manera similar.

La vigilancia de Internet a menudo involucra la cooperación de los proveedores de telecomunicaciones con las agencias de inteligencia, a quienes les entregan copias de todo lo que pasa por sus conmutadores. La NSA es una experta en esto, ya que recopila los datos que circulan por las fronteras de Estados Unidos e internacionalmente mediante acuerdos con países socios. Sabemos que la NSA instala equipos de vigilancia en los conmutadores de

AT&T dentro de Estados Unidos y que ha recopilado metadatos de teléfonos móviles de Verizon y de otros. Del mismo modo, Rusia tiene acceso masivo a los datos de los proveedores de red dentro de sus fronteras.[43]

La mayoría de los países no tiene ni el presupuesto ni la experiencia para desarrollar este tipo de herramientas de vigilancia y piratería, sino que, por el contrario, se las compran a los fabricantes de armas cibernéticas.[44] Compañías como el Grupo Gamma de FinFisher (Alemania y el Reino Unido), HackingTeam (Italia), VASTech (Sudáfrica), Cyberbit (Israel) y NSO Group (también de Israel) les venden estas herramientas a países como los enumerados más arriba, lo que les permite piratear ordenadores, teléfonos y otros dispositivos. Incluso tienen una conferencia, llamada ISS World y conocida como *el baile de los pinchadores de teléfonos*, en la que venden explícitamente sus productos a regímenes represivos con este propósito.[45]

Durante el tiempo que Internet ha estado presente, su vigilancia se ha utilizado con fines de espionaje en el extranjero. La NSA habrá liderado el camino, pero otros países no estaban muy lejos. Las primeras operaciones de espionaje contra Estados Unidos incluyeron Moonlight Maze en 1999 (probablemente por parte de Rusia),[46] Titan Rain, a principios de 2000 (casi con certeza de China),[47] y Buckshot Yankee en 2008 (no tenemos ni idea de quién estaba detrás de esta).[48]

Los chinos han llevado a cabo operaciones de ciberespionaje contra el Gobierno de Estados Unidos durante décadas: a lo largo de los años, han robado planos y documentos de diseño de varios sistemas de armas, incluido el avión de combate F-35;[49] en 2010, piratearon a Google para acceder a las cuentas de Gmail de activistas taiwaneses;[50] en 2015, nos enteramos de que estaba accediendo a las cuentas de correo electrónico de los principales funcionarios del Gobierno de Estados Unidos[51] y también, en 2015, piratearon la Oficina de Administración de Personal estadounidense y robaron archivos personales detallados de todos los ciudadanos del país con autorización de seguridad, entre otros.[52]

Durante la última década, las compañías de antivirus han expuesto sofisticadas herramientas de piratería y vigilancia de Rusia,[53] China,[54] Estados Unidos,[55] Estados Unidos e Israel juntos,[56] España y varios países no identificados.[57] En 2017, Corea del Norte atacó a los militares de Corea del Sur y les robó planes de contingencia clasificados de tiempos de guerra.[58]

Esto no es solo inteligencia política o militar, sino el robo generalizado de propiedad intelectual de corporaciones por parte de otros Gobiernos. China,

por ejemplo, ha robado tanta propiedad intelectual comercial de Estados Unidos que el espionaje fue uno de los temas clave de discusión entre el presidente Obama y el presidente chino Xi Jinping en 2015, cuando los dos países llegaron a un acuerdo para terminar con él.[59] (Como resultado, China parece haber atenuado su ciberespionaje económico)[60].

Todo esto se considera normal. El espionaje es una actividad legítima en tiempos de paz, y por lo general los países pueden hacer lo que les permita salirse con la suya. Justo cuando la NSA espiaba el teléfono inteligente de la canciller alemana Angela Merkel, otra persona hacía lo mismo con el teléfono del jefe de personal de la Casa Blanca John Kelly.[61] A pesar de que la violación de la OPM afectó a 21,5 millones de estadounidenses, en realidad no pudimos condenar a China, porque los estadounidenses hacemos lo mismo. De hecho, James Clapper, el director de Inteligencia Nacional, dijo en aquel momento lo siguiente: «Hay que felicitar a los chinos por lo que hicieron».[62]

El país cuyas actividades conocemos más es Estados Unidos. La NSA es en sí misma una clase aparte por varias razones: su presupuesto es significativamente mayor que el de cualquier organismo comparable en el planeta;[63] la mayoría de las grandes empresas de tecnología del mundo están ubicadas dentro de Estados Unidos o en uno de sus países socios, lo que ofrece un mayor acceso a sus datos; la ubicación física de los principales cables de Internet del planeta hace que muchas de las comunicaciones del mundo pasen por Estados Unidos en algún momento,[64] y, por último, la NSA tiene acuerdos secretos con otros países para un acceso aún más amplio a las redes de comunicaciones del planeta.

La policía estadounidense también se encarga de la vigilancia, pero no tiene nada que ver con lo que hace la NSA, sino que se rige por un conjunto de leyes diferente y más restrictivo, y tienen que seguir los procedimientos legales en relación con la búsqueda y la incautación. Podemos discutir si tales leyes están bien elaboradas y si la policía las sigue de forma diligente, pero sí es cierto que tienen consecuencias importantes. La policía debe dirigir su vigilancia a sospechosos individuales, mientras que la NSA no lo hace. La policía necesita reunir evidencias que sean admisibles en un tribunal; la NSA no lo necesita. La aplicación de la ley por lo general sucede después de que haya ocurrido un crimen; la NSA lleva a cabo el espionaje mientras las actividades están en curso.

Algunos países llevan la vigilancia hasta el extremo y utilizan Internet para espiar a toda su población. China lleva la delantera: todas las plataformas

de medios sociales del país están controladas por el Gobierno, quien puede censurar las declaraciones ofensivas.[65] (La meta del Gobierno no es limitar el discurso, sino la capacidad de crear movimientos sociales, organizar protestas y cosas por el estilo.)[66]

Aparte de para la vigilancia, muchos países utilizan Internet para censurar y controlar a sus ciudadanos. Los Gobiernos autoritarios vieron la Primavera Árabe y las revoluciones coloridas de principios de la década de 2000 como una amenaza existencial, y creen que este tipo de control es esencial para la supervivencia del régimen. Países como Rusia, China e Irán procesan directamente a las personas que publican ciertos materiales, obligan a las empresas a censurarlos u orientan las discusiones en línea en direcciones inocuas. Aquí también China toma la delantera. Cuenta con el régimen de censura más extenso de todos los países: su gran cortafuegos es un sistema integral diseñado para limitar el acceso a Internet global desde el interior del país.[67] En 2020, planea implementar un sistema de crédito social: cada ciudadano recibirá una puntuación basada en todas sus actividades vigiladas que se utilizará como puerta de acceso a varios derechos y privilegios.[68] Y China exporta su experiencia en control social a otros países totalitarios.

No obstante, no toda la censura es nefasta. Francia y Alemania censuran el discurso nazi;[69] muchos países, las violaciones de los derechos de autor, y prácticamente todos, la pornografía infantil.

Para lograr todo este espionaje, vigilancia y control, los Estados nación están haciendo uso de las inseguridades de Internet, de lo que hablaremos en el capítulo 9. Esto no va a desaparecer pronto y seguirá siendo una de las fuerzas impulsoras detrás de las políticas de seguridad del Internet+ de los países.

LA GUERRA CIBERNÉTICA ES LO NORMAL

Unos dicen que la guerra cibernética está llegando,[70] otros que ya está aquí[71] y algunos que está en todas partes.[72] En realidad, *guerra cibernética* es un término que todos usan, con el que nadie está de acuerdo y que no tiene una definición común.[73] Sea cual sea el término, los países utilizan la inseguridad inherente de Internet para atacarse unos a otros; priorizan la capacidad de atacar por encima de la capacidad de defenderse, lo que ayuda a perpetuar un Internet inseguro para todos nosotros.

Stuxnet, descubierta en 2010, fue un arma sofisticada desarrollada por Estados Unidos e Israel para atacar la planta de armas nucleares de Natanz en

Irán.[74] Se dirigió contra una marca de Siemens de controladores lógicos programables que automatizan los equipos de fábrica, como las centrífugas utilizadas para enriquecer el uranio de calidad de las armas. Se propagó a través de ordenadores con Windows buscando controladores de centrífuga específicos de Siemens. Cuando los encontró, los aceleró y ralentizó en varias ocasiones, lo que provocó que se destruyeran a sí mismos, al mismo tiempo que ocultaban a los operadores lo que estaban haciendo.

Militares y agencias de inteligencia nacionales en todo Internet acceden a ordenadores extranjeros y, en algunos casos, están causando daños tanto virtuales como físicos. Las reglas y normas internacionales sobre lo permitido y lo que sería una respuesta justa y proporcional permanecen en su mayoría indefinidas. Este entorno favorece el ataque sobre la defensa, de igual forma que la tecnología de seguridad de Internet hace que el ataque sea más fácil que la defensa. Y las dinámicas son muy diferentes a las de la guerra convencional.

Los objetivos no se limitan a las áreas y sistemas militares, sino que se extienden a emplazamientos industriales dedicados a la producción de petróleo, el procesamiento químico y la fabricación, y la generación de energía, todos ellos controlados ahora a través de Internet.[75]

Un ciberataque puede ser parte de una operación más grande. En 2007, Israel atacó una planta nuclear siria,[76] aunque no fue un ataque cibernético, ya que aviones de guerra convencionales bombardearon el lugar, pero sí hubo un componente cibernético: antes de que los aviones despegaran, los piratas informáticos israelíes hackearon los sistemas de radar y antiaéreos en Siria y los países vecinos para desactivarlos. En 2008, Rusia coordinó operaciones convencionales y cibernéticas en un ataque contra Georgia.[77] Estados Unidos realizó una serie de operaciones cibernéticas durante la guerra de Irak de 1990-1991.[78] En 2016, el presidente Obama reconoció que Estados Unidos estaba realizando operaciones cibernéticas como parte de su ofensiva más grande contra ISIS.[79]

A veces los ataques son exploratorios o preparatorios. En 2017, nos enteramos de que un grupo de hackers rusos habían irrumpido en al menos veinte redes de compañías eléctricas en Estados Unidos y Europa, y en algunos casos lograron deshabilitar el sistema.[80] En 2016, los iraníes hicieron lo mismo en una presa en el estado de Nueva York.[81] Los expertos suponen que estas operaciones fueron de reconocimiento para posibles acciones futuras,[82] lo que se conoce como *preparar el terreno*, y parece que muchos países lo están haciendo.[83]

Los riesgos han aumentado conforme nuestro mundo se ha vuelto más informatizado, más conectado en red y más estandarizado. Durante la Guerra Fría, la mayoría de los ordenadores militares y los sistemas de comunicaciones eran distintos de sus homólogos civiles, pero nada más. Millones de ordenadores del Departamento de Defensa ejecutan Windows, incluidos los que controlan los sistemas de armas. Los mismos ordenadores y redes que tienes en tu hogar y oficina controlan la infraestructura crítica de casi todos los países. Esto convierte a Internet en un objetivo potencial.

No se trata solo de las potencias más fuertes contra las más débiles, como sucedió con Rusia cuando atacó las redes de Estonia en 2007,[84] las de Georgia en 2008 y las de Ucrania en varias ocasiones. Un Estado nación más pequeño puede infligir daños desproporcionados a su objetivo en el ciberespacio por muchas de las razones discutidas en el capítulo 1; por ejemplo, el Ejército Electrónico Sirio atacó sitios de noticias de Estados Unidos en 2013, e Irán atacó el hotel Sands de Las Vegas en 2014.[85]

Las capacidades de cada país varían mucho. En el extremo superior están aquellos con comandos cibernéticos militares y agencias de inteligencia totalmente desarrolladas que pueden crear sus propias herramientas de ataque personalizadas. Aquí encontramos a Estados Unidos, el Reino Unido, Rusia, China, Francia, Alemania e Israel.[86] Están bien financiados, son muy hábiles y no son fáciles de disuadir. Son la élite, aunque la mayoría de sus operaciones cibernéticas no son sofisticadas porque la seguridad suele ser tan mala que no les hace falta.[87] En un nivel inferior se sitúan los países que compran herramientas y servicios comerciales a los fabricantes de armas cibernéticas mencionados con anterioridad. Y aún más abajo están los países que simplemente usan software de piratería criminal descargado de Internet. Los países de estos últimos niveles también pueden contratar mercenarios cibernéticos.[88] El aumento de las capacidades parece requerir algo más que convertirlo en una prioridad. Si un país aislado y fuertemente sancionado, como Corea del Norte, puede pasar de ser una no-entidad en el ciberespacio a una amenaza significativa en menos de una década, cualquiera puede hacerlo.[89]

Los riesgos del ataque cibernético de los Estados nación están aumentando, y los Gobiernos están tomando nota. Todos los años, el director de Inteligencia Nacional de Estados Unidos presenta una evaluación de la amenaza mundial al Senado y al Comité Selecto de Inteligencia de la Cámara. Es una buena guía para lo que nos preocupa. El documento de 2007 no menciona en absoluto las amenazas cibernéticas.[90] Incluso en el informe de

2009, «la creciente amenaza cibernética y del crimen organizado» solo se discutió al final del documento, lo que parecía más bien una ocurrencia tardía.[91] En cambio, en el año 2010, la cibernética fue la primera amenaza enumerada en el informe anual,[92] y desde entonces se pinta cada vez en términos más terribles. Del informe de 2017 extraemos el siguiente fragmento:[93]

> Nuestros adversarios se están volviendo más adeptos al uso del ciberespacio para amenazar nuestros intereses y promover los suyos, y a pesar de mejorar las defensas cibernéticas, casi toda la información, las redes de comunicación y los sistemas estarán en riesgo durante años.
>
> Las amenazas cibernéticas ya están desafiando la confianza de la sociedad y la confianza en las instituciones globales, el Gobierno y las normas mientras imponen costes a las economías de Estados Unidos y globales. Las amenazas cibernéticas también representan un riesgo cada vez mayor para la salud pública, la seguridad y la prosperidad, ya que las tecnologías cibernéticas se integran con la infraestructura crítica en sectores clave. Estas amenazas se amplifican con nuestra actual delegación de toma de decisiones, detección y autenticación en sistemas automatizados potencialmente vulnerables. Esta delegación aumenta las posibles consecuencias físicas, económicas y psicológicas de los ataques cibernéticos y los casos de explotación cuando ocurren.

De manera similar, la Conferencia de Seguridad de Múnich (la conferencia internacional sobre política de seguridad más importante del mundo) no tuvo un panel sobre ciberseguridad hasta 2011.[94] Ahora la ciberseguridad tiene su propio evento.

Todos estamos dentro del radio de influencia. Incluso un arma cibernética bien dirigida, como Stuxnet, dañó redes muy lejos de la planta nuclear iraní de Natanz.[95] En 2017, el gigante naviero mundial Maersk tuvo que detener sus operaciones por culpa de NotPetya, un arma cibernética rusa utilizada contra Ucrania;[96] la compañía era un espectador atrapado en el fuego cruzado de un ataque cibernético internacional.

Hasta ahora, la mayoría de los ataques cibernéticos no han ocurrido en tiempos de guerra. No hubo guerra cuando Estados Unidos e Israel atacaron a Irán con Stuxnet en 2010, ni cuando Irán atacó a la compañía petrolera nacional saudí en 2012.[97] No hubo guerra cuando Corea del Norte usó WannaCry para bloquear los sistemas informáticos de todo el mundo en 2017,

ni en los años anteriores, cuando Estados Unidos llevó a cabo operaciones cibernéticas contra Corea del Norte tratando de sabotear su programa nuclear.[98] En 2012, un general ruso de alto rango publicó un artículo explicando lo que se conoció como doctrina Gerasimov, que reclamaba «el uso de fuerzas de operaciones especiales y la oposición interna para crear un frente operativo permanente», incluida la participación en «acciones de larga distancia sin contacto directo contra el enemigo» a través de «acciones informáticas, dispositivos y medios».[99] Esto se parece mucho a la piratería rusa del proceso electoral de 2016 en Estados Unidos. En el mundo de hoy, las líneas entre la guerra y la paz son borrosas, y las tácticas secretas, como las operaciones cibernéticas analizadas en este capítulo, se han vuelto más importantes. Otros países parecen estar de acuerdo. Es por eso por lo que algunos dicen que ya estamos involucrados en una guerra cibernética.

Hay ciberataques que se considerarán actos de guerra. Estados Unidos ha declarado que cualquier respuesta a tales ataques no estará necesariamente limitada al ciberespacio.[100] Sin embargo, la mayoría de las acciones ofensivas en el ciberespacio se han llevado a cabo en una zona gris entre la paz y la guerra (un estado que el científico político Lucas Kello llama de *no paz*),[101] donde nadie está seguro de cómo responder. Estados Unidos respondió al ataque de Corea del Norte contra Sony con algunas sanciones menores[102] y al pirateo ruso de las elecciones de 2016 cerrando los consulados y expulsando a los diplomáticos.[103] La mayoría de los países responden a los ataques con duras palabras, y ya está.

Hay varias razones para esto. La primera es que no hay una línea bien definida entre lo que se considera un acto de guerra y lo que no. El espionaje internacional suele considerarse una actividad válida en tiempos de paz, y matar a un gran número de personas, un acto de guerra. Todo lo demás está en el medio.

Como decía en el capítulo 3, la atribución puede ser difícil. En particular, hay una participación continua del Gobierno en ataques cibernéticos. El experto en políticas cibernéticas Jason Healey desarrolló un espectro completo que iba desde los ataques alentados por el Estado hasta los coordinados y ejecutados por este, con muchos otros matices de participación en el medio.[104] Por tanto, incluso aunque pueda atribuirse un ataque a una ubicación geográfica concreta, es complicado determinar si un Gobierno es responsable y en qué medida.

La razón última por la que las respuestas a los ataques tienden a ser silenciosas es que es difícil distinguir, hasta que es demasiado tarde, la

diferencia entre el ciberespionaje y el ciberataque (pues, hasta el último segundo, que un intruso no autorizado lo copie todo o dispare una carga útil destructiva parece lo mismo).

Los ciberataques militares han sido en gran medida ineficaces a largo plazo. El espionaje es fácil y los efectos a corto plazo, dañinos pero fugaces, como un apagón en Ucrania; pero cualquier otra cosa parece ser difícil. Aunque Stuxnet tuvo éxito, en el mejor de los casos frenó a Irán un par de años y consiguió un efecto mínimo en cualquier negociación internacional. Estados Unidos también utilizó ataques cibernéticos para frustrar a Corea del Norte en sus intentos de construir un arma atómica y un sistema de entrega. De nuevo, las operaciones tuvieron muy pocas repercusiones a largo plazo. [105] Las armas cibernéticas se utilizaron en el reciente conflicto armado con Ucrania, así como en la guerra civil de Siria, donde, una vez más, los efectos fueron mínimos.[106]

Unos cuantos temas más enfatizan la importancia y la prevalencia del ataque sobre la defensa en el arte bélico cibernético moderno. Las armas cibernéticas son únicas porque son inherentemente inestables; es decir, si tienes un arma cibernética que usa una cierta vulnerabilidad para funcionar, puedo desactivarla encontrándola y parcheándola, lo que significa que un país que se encuentre con una ventaja temporal tendrá que sopesar los riesgos de lanzar un ataque preventivo frente a los riesgos de que su arsenal se agote debido a la investigación defensiva en curso.[107] Esta inestabilidad hace que las armas cibernéticas sean más atractivas de usar; de usar ahora, antes de que se descubran por otro lado.

Las armas cibernéticas pueden robarse y usarse de una forma que las armas convencionales no pueden. En 2009, China filtró los planos y otros datos del avión de combate F-35 de Estados Unidos de Lockheed Martin y varios subcontratistas. Si bien el robo de propiedad intelectual sin duda le ahorró al Gobierno chino parte de los 50.000 millones de dólares que Estados Unidos gastó en el desarrollo, así como muchos años de esfuerzo, el ejército chino todavía tenía que diseñar y construir los aviones.[108] Por el contrario, los atacantes que robaron armas cibernéticas tanto de la NSA como de la CIA pudieron usarlas con muy poco tiempo y coste adicionales. Y cuando esas herramientas de piratería se filtraron al público, tanto los Gobiernos extranjeros como los delincuentes las utilizaron de inmediato para sus propios fines.

Los países también se están volviendo más descarados en sus ofensivas. [109] Los ataques continuos contra Estados Unidos por parte de Rusia, China y

Corea del Norte, así como los ocasionales de Irán, Siria y otros, demuestran que pueden actuar con impunidad.

Siendo honestos, Estados Unidos solo puede culparse a sí mismo. Priorizamos la ofensiva sobre la defensa, fuimos los primeros en utilizar Internet tanto para el espionaje como para el ataque y minamos la confianza en las compañías de tecnología estadounidenses a través de la NSA. Hemos traspasado los límites de lo que es aceptable. Como sentimos que teníamos una ventaja sobre otros países, no intentamos negociar ningún tratado ni establecer normas y, al mismo tiempo, desarrollamos Internet como un espacio comercial donde la seguridad era una idea improvisada, o ni eso. Fuimos cortos de miras y ahora nuestras acciones se están volviendo contra nosotros.

El resultado es lo que los expertos en política exterior llaman *dilema de seguridad*. El ataque no solo es más fácil que la defensa, sino más barato.[110] Así que, si un país quiere volverse más poderoso en el ciberespacio, sería más inteligente que invirtiera en su ofensiva (lo que significa usar la inseguridad inherente a Internet). Pero, si todo el mundo hiciera eso, el planeta se volvería menos estable e Internet aún menos seguro. Esta es la batalla de la guerra cibernética en la que se encuentran los países en este momento.

Las democracias occidentales son los países más vulnerables del planeta y los menos preparados para el ciberataque, aunque esto no quiere decir que otros no deban preocuparse. Sir John Sawers, el exjefe del MI6 del Reino Unido, dijo esto en 2017: «Creo que tanto China como Estados Unidos, y probablemente Rusia también, se sienten vulnerables a ser atacados, en lugar de sentir el poder de atacarse entre ellos».[111]

Como el reportero de seguridad nacional Fred Kaplan dijo, refiriéndose a Estados Unidos: «Tenemos mejores ciberrocas para tirar a las casas de otros países, pero nuestra casa tiene más ventanas que las de ellos».[112] Hablaremos mucho más sobre esto en el capítulo 9.

La conclusión es que los países se encuentran en este nuevo estado perpetuo de falta de paz, en el que las reglas de compromiso aún no están escritas y todo está desequilibrado y es desconocido. Las principales potencias, todas las que perciben su propia vulnerabilidad, son naturalmente reacias a dejar sus armas cibernéticas, las cuales dependen de las vulnerabilidades en Internet. Para preservar y mejorar sus capacidades ofensivas en este desconocido teatro de guerra, trabajan con diligencia para perpetuar la inseguridad. Hablaré más sobre cómo hacen esto, por qué su

lógica es incorrecta y qué deben hacer para revertir el curso en los capítulos 9 y 10.

LOS BENEFICIOS CRIMINALES DE LA INSEGURIDAD

Por supuesto que los criminales prefieren un Internet inseguro: es más rentable para ellos.

El famoso Willie Sutton robó a los bancos porque «ahí es donde está el dinero». Hoy el dinero está en línea y, cada vez más, los criminales también. Los delincuentes roban dinero de nuestras cuentas bancarias, los datos de nuestra tarjeta de crédito —que utilizan para cometer un fraude— o información sobre nuestra identidad para usarla. También bloquean nuestros datos y luego tratan de obligarnos a pagar su devolución —ransomware.

En 2018, el hospital de Indiana Hancock Health fue víctima de un ataque cibernético. Los delincuentes (no tenemos idea de quiénes eran) cifraron sus ordenadores y exigieron 55.000 bitcoins para desbloquearlos. El personal médico no tenía acceso a registros médicos informatizados. Aunque contaban con copias de seguridad, temían que la recuperación de los datos pusiera en riesgo a los pacientes. Pagaron.[113]

El ransomware es cada vez más común y lucrativo.[114] Las víctimas van desde organizaciones, como en la historia anterior, a individuos. El laboratorio Kaspersky informó de que los ataques a empresas se triplicaron, y el número de variantes diferentes de ransomware se multiplicó por once en nueve meses en 2016.[115] Symantec encontró que las cantidades promedio de rescate se incrementaron de 294 dólares en 2015 a 679 en 2016 y a más de 1.077 en 2017.[116] Carbon Black informó de que las ventas totales de software de ransomware en el mercado negro aumentaron 25 veces de 2016 a 2017, a 6,5 millones de dólares.[117] El ransomware ahora viene con instrucciones detalladas para poder pagar y algunos incluso tienen líneas de ayuda telefónica para ayudar a las víctimas. (Si estás pensando que una línea de ayuda es peligrosa para los delincuentes, recuerda la naturaleza internacional de todo esto. Los delincuentes no temen que los procesen en sus países de origen). Después de todo, es un negocio de mil millones de dólares.[118]

La ciberdelincuencia es una gran empresa global que genera entre 500.000 millones[119] y 3 billones de dólares[120] al año, dependiendo de en qué análisis te bases. Se cree que las pérdidas adicionales debidas al robo de

propiedad intelectual cuestan entre 225 y 600.000 millones de dólares cada año.[121]

Gran parte de la ciberdelincuencia implica una suplantación de la identidad: sabotear los sistemas de autenticación analizados en el capítulo 3. Entrar en un banco fingiendo ser otra persona es una forma peligrosa de ganar dinero, pero hacer lo mismo en la página web de un banco es mucho más fácil y menos arriesgado. Con frecuencia lo único que se necesita para delinquir es el nombre de usuario y la contraseña de la víctima. No es diferente con las tarjetas de crédito: si un delincuente tiene el número de tarjeta de la víctima y otra información (nombre, dirección, lo que sea), puede usar la tarjeta para lo que quiera. Esto es robo de identidad; tiene muchas variantes, todas basadas en credenciales robadas y suplantación de identidad.

El fraude del CEO, o compromiso de correo electrónico comercial, es una modalidad específica de robo de identidad. Un ladrón finge ser el director general de una empresa u otro ejecutivo y manda un correo electrónico al departamento de cuentas por pagar diciéndoles que envíen un cheque al delincuente,[122] o que envíen una copia del formulario de las nóminas y retenciones de cada empleado, como precursor para presentar una declaración de impuestos falsa o para desviar las ganancias de una venta de bienes raíces.[123] Esto puede ser muy efectivo si el criminal investiga: todos estamos acostumbrados a tratar los correos electrónicos del jefe como auténticos e importantes.

Pero hay más. Una gran cantidad de delitos informáticos se derivan de esta pregunta: he pirateado todos estos ordenadores, ¿qué puedo hacer con ellos? Resulta que la respuesta es: bastante.[124] Los delincuentes han aprovechado un gran número de ordenadores pirateados en redes robot o zombis. Las botnets pueden usarse para todo tipo de cosas: enviar spam en grandes cantidades, resolver CAPTCHA y extraer bitcoins.[125] Los piratas informáticos utilizan robots para cometer fraudes de clics: hacen clic repetidamente en los anuncios de los sitios que controlan y obtienen ingresos de los terceros que los colocan, o hacen clic en los anuncios publicados por los competidores y los obligan a pagar.[126] Usan botnets masivas para lanzar ataques DDoS (ataque de negación de servicio distribuido, por sus siglas en inglés) contra otras víctimas.

Si controlas millones de robots, puedes usarlos para acabar con las conexiones de Internet de particulares e incluso de empresas y echarlos de una patada de Internet. Es difícil defenderse de este tipo de ataques, dada su magnitud, aunque la tubería de datos del defensor sea lo bastante grande

como para manejar todo el tráfico entrante. A veces los atacantes extorsionan dinero de compañías con una amenaza.

Las organizaciones criminales internacionales explotan las lagunas legales y jurisdiccionales en todo el mundo. Venden herramientas de ataque e incluso ofrecen crimeware como servicio, también conocido como CaaS (por sus siglas en inglés). Según la Interpol:

> El modelo CaaS proporciona un fácil acceso a herramientas y servicios en todo el espectro de la criminalidad, desde jugadores de nivel muy básico hasta jugadores de primer nivel, incluidos aquellos con otras motivaciones, como los hacktivistas e incluso los terroristas. Esto permite que incluso los cibercriminales de nivel básico realicen ataques a una escala desproporcionada a su capacidad técnica.[127]

Los delincuentes individuales se especializan en robo de credenciales, fraude de pagos y blanqueo de dinero; venden herramientas de hackeo y ofrecen servicios de botnets.[128] Incluso hay algunos Gobiernos que participan en actividades delictivas y otros que hacen la vista gorda con los delincuentes que operan a nivel internacional en sus países. El caso de Corea del Norte es particularmente escandaloso:[129] emplea a hackers para recaudar dinero para las arcas del Gobierno,[130] y, en 2016, robó 81 millones de dólares del banco de Bangladesh.[131]

Por supuesto, el lucro no es la única motivación criminal. La gente comete crímenes por odio, miedo, venganza, por razones políticas y por muchos otros motivos. Es difícil encontrar datos sobre qué porcentaje del crimen total no es financiero. Sabemos que las personas cometen con frecuencia tales crímenes, y cada vez más lo hacen en Internet: acoso cibernético, robo y publicación de información personal para obtener beneficios políticos o por despecho y para causar daño.

Cada día se utilizan más ordenadores para piratear y controlar, y hay más datos para robar. Ya lo estamos comprobando. Hemos visto cámaras web, DVR y rúters domésticos pirateados, que forman parte de redes de robots informáticos, utilizados para lanzar ataques DdoS;[132] electrodomésticos, como frigoríficos, que se han usado para enviar correos electrónicos no deseados,[133] o atacantes que han bloqueado los dispositivos del IoT, lo que los hace inservibles de forma permanente.[134]

Todavía no hemos experimentado asesinatos cometidos a través de Internet, pero existe la posibilidad. En 2007, el desfibrilador cardíaco del entonces vicepresidente Dick Cheney se modificó expresamente para

dificultar su asesinato;[135] en 2017, un hombre envió un tuit diseñado para provocar un ataque en un destinatario epiléptico,[136] y ese mismo año WikiLeaks publicó información acerca del trabajo de la CIA sobre el pirateo remoto de automóviles.[137]

El ransomware también está llegando al Internet de las cosas. Los ordenadores integrados no son más resistentes a este tipo de software que tu portátil, y los delincuentes ya son conscientes de que una defensa obvia contra el ransomware informático —restaurar los datos desde la copia de seguridad — no funcionará cuando las vidas corran un riesgo inmediato. Los piratas informáticos han probado la existencia de ransomware en termostatos inteligentes[138] y, en 2017, a un hotel austríaco le piratearon las cerraduras electrónicas de las puertas y las retuvieron para conseguir un rescate.[139] Automóviles, dispositivos médicos, electrodomésticos y todo aquello a lo que puedan llegar los hackers es lo siguiente. El potencial de ingresos adicionales provenientes del crimen es enorme.

También lo es el potencial para causar daños graves. Un coche bloqueado que exige doscientos dólares en bitcoins es un inconveniente caro; una petición similar a gran velocidad es potencialmente mortal. Pasa lo mismo con los dispositivos médicos. En 2017, el ransomware NotPetya cerró hospitales en Estados Unidos y Reino Unido;[140] en algunos casos, los hospitales del Reino Unido quedaron tan incapacitados que tuvieron que retrasar las cirugías,[141] enviar a los pacientes de emergencia a otros lugares[142] y reemplazar el equipo médico dañado. En los próximos años veremos cómo los ataques se dirigirán sobre todo a dispositivos del IoT y a otros ordenadores integrados. Presagiamos esto con el caso de la botnet Mirai en 2016,[143] que acopló una gran variedad de dispositivos del IoT en la red zombi más grande del mundo, y aunque no se usó para difundir ransomware, podría haberse hecho con facilidad.

05

LOS RIESGOS SE TORNAN CATASTRÓFICOS

LAS TENDENCIAS DE LOS CUATRO capítulos anteriores no son nuevas; ni las realidades técnicas, ni las tendencias políticas y económicas. Nada. Lo que está cambiando es cómo se utilizan los ordenadores en la sociedad: la magnitud de sus decisiones, la autonomía de sus acciones y su interacción con el mundo físico. Esto aumenta la amenaza en muchas otras dimensiones.

LOS ATAQUES DE INTEGRIDAD Y DISPONIBILIDAD ESTÁN AUMENTANDO

La seguridad en la información suele describirse como una tríada consistente en confidencialidad, integridad y disponibilidad. Verás que se conoce como *tríada de la* CIA,[1] lo cual es confuso en el contexto de la seguridad nacional. Pero básicamente las tres cosas que puedo hacer con tus datos son robar una copia, modificarla o eliminarla.

Hasta ahora las amenazas han sido en gran parte referentes a la confidencialidad. Este tipo de ataques pueden ser costosos, como cuando los norcoreanos piratearon a Sony en 2014; embarazosos, como el robo de fotos de celebridades del iCloud de Apple en 2014[2] o la violación de la web para adultos Ashley Madison en 2015;[3] perjudiciales, como cuando los rusos piratearon al Comité Nacional Demócrata en 2016[4] o cuando hackers sin nombre robaron 150 millones de registros personales de Equifax en 2017,[5] e incluso pueden suponer una amenaza para la seguridad nacional, como en el caso de la filtración de datos de la Oficina de Gestión de Personal de 2015.[6] Todas ellas son violaciones de confidencialidad.

Sin embargo, una vez que se les da a los ordenadores la capacidad de afectar al mundo, las amenazas de integridad y disponibilidad son más importantes. La manipulación de la información es una amenaza creciente a medida que los sistemas se vuelven más capaces y autónomos. La denegación de servicio es un riesgo cada vez mayor porque los sistemas se están

volviendo esenciales. La piratería es una amenaza que va en aumento, ya que los sistemas tienen implicaciones para la vida y la propiedad. Mi coche tiene conexión a Internet, y, aunque me preocupa que alguien pueda piratearlo y escuchar mis conversaciones mediante la conexión bluetooth (una amenaza de confidencialidad), me preocupa mucho más que desactiven los frenos (una amenaza de disponibilidad) o modifiquen los parámetros de los sistemas automáticos de seguimiento a distancia y de mantenimiento en carril (una amenaza a la integridad). La amenaza de confidencialidad afecta mi privacidad; las amenazas de disponibilidad e integridad pueden matarme. Lo mismo sucede con las bases de datos. Me preocupa la privacidad de mis registros médicos, pero más aún que alguien pueda cambiar mi tipo de sangre o lista de alergias (una amenaza a la integridad) o apagar equipos que salvan vidas (una amenaza de disponibilidad). Una forma de pensar sobre esto es que las amenazas de confidencialidad tienen que ver con la privacidad, pero las amenazas de integridad y disponibilidad afectan en realidad a la seguridad.[7]

Los sistemas más grandes también son vulnerables. En 2007, el Laboratorio Nacional de Idaho evidenció un ataque cibernético contra una turbina industrial, lo que causó que se descontrolara y se destruyera.[8] En 2010, Stuxnet hizo lo mismo con las centrífugas nucleares iraníes. En 2015, hackearon una fábrica de acero sin nombre en Alemania e interrumpieron los sistemas de control, por lo que un alto horno no pudo cerrarse adecuadamente y provocó un daño enorme.[9] Y, en 2016, el Departamento de Justicia estadounidense acusó a un hacker iraní que accedió a la presa Bowman en Rye (Nueva York); según los cargos, era capaz de operar de forma remota en las compuertas de la presa, y, aunque no hizo nada con este acceso, pudo haberlo hecho.[10]

Estos son los sistemas de control industrial conocidos como SCADA. Nuestras presas, centrales eléctricas, refinerías de petróleo, plantas químicas y todo lo demás están en Internet y son vulnerables, y debido a que todos ellos afectan al mundo directa y físicamente, los riesgos aumentan de forma drástica.

Estos sistemas fallarán, y algunas veces gravemente. Fallarán por accidente y bajo ataque. El sociólogo Charles Perrow estudia la complejidad y los accidentes, y a modo de profecía escribía en 1984:

> Los accidentes y, por lo tanto, las catástrofes potenciales son inevitables en sistemas complejos estrechamente relacionados y pueden ser letales. Debemos esforzarnos más en reducir los errores, y eso ayudará mucho, pero para algunos sistemas no será suficiente […].

> Debemos vivir y morir con sus riesgos, apagarlos o rediseñarlos por completo.[11]

En 2015, un joven de dieciocho años equipó un dron con una pistola para un proyecto de ciencias y publicó el vídeo en YouTube de esa pistola disparando con control remoto.[12]

Esta es solo una manera posible de usar Internet+ para cometer un asesinato. También alguien podría tomar el control de un vehículo a toda velocidad,[13] hackear una bomba dosificadora de un hospital y proporcionarle a la víctima una dosis letal de un medicamento[14] o comprometer los sistemas eléctricos durante una ola de calor. Estas no son preocupaciones teóricas, sino que investigadores de seguridad han demostrado la posibilidad de que ocurran.

Los coches son vulnerables; también lo son los aviones,[15] los barcos comerciales,[16] las señales de tráfico electrónicas[17] y las sirenas de tornado.[18] Los sistemas de armas nucleares son seguramente vulnerables a los ataques cibernéticos,[19] de la misma manera que lo son los sistemas electrónicos que advierten a las personas sobre ellos, y también los satélites.[20]

Para que la sociedad funcione, debemos confiar en los procesos informáticos que afectan a nuestras vidas,[21] pero los ataques contra la integridad de los datos socavan esta confianza. Hay muchos ejemplos: en 2016, piratas informáticos del Gobierno ruso irrumpieron en la Agencia Mundial Antidopaje y modificaron los datos de las pruebas de drogas de los atletas,[22] y, en 2017, unos hackers, posiblemente contratados por el Gobierno de los Emiratos Árabes Unidos, piratearon una agencia de noticias en Catar y publicaron citas incendiarias, falsamente atribuidas al emir del país, elogiando a Irán y a Hamás y precipitando una crisis diplomática entre Catar y sus vecinos.[23]

Hay evidencias de que los rusos accedieron a las bases de datos de los votantes en veintiún estados de Estados Unidos en vísperas de las elecciones de 2016.[24] Las consecuencias fueron mínimas, pero un ataque a la integridad o a la disponibilidad más extenso habría sido devastador.

Así lo expresaba en la *Evaluación mundial de amenazas* de 2015 el director de Inteligencia Nacional de Estados Unidos:

> La mayor parte de la discusión pública sobre las amenazas cibernéticas se ha centrado en la confidencialidad y la disponibilidad de la información; el ciberespionaje socava la confidencialidad, mientras que

> las operaciones de denegación de servicio y los ataques de eliminación de datos socavan la disponibilidad. Sin embargo, en el futuro también podremos ver más operaciones cibernéticas que cambiarán o manipularán la información electrónica para comprometer su integridad (es decir, precisión y confiabilidad) en lugar de eliminarla o interrumpir el acceso a ella. La toma de decisiones por parte de altos funcionarios gubernamentales (civiles y militares), ejecutivos corporativos, inversores u otros se verá afectada si no pueden confiar en la información que están recibiendo.[25]

En testimonios independientes ante varios comités de la Cámara y el Senado estadounidenses que dieron en 2015, el director de Inteligencia Nacional James Clapper[26] y el director de la NSA Mike Rogers[27] hablaron sobre este tipo de amenazas. Las consideran mucho más serias que la amenaza de confidencialidad y creen que Estados Unidos es vulnerable.

La *Evaluación mundial de amenazas* de 2016 describe la amenaza de la siguiente manera:

> Es probable que las operaciones cibernéticas futuras incluyan un mayor énfasis en cambiar o manipular los datos para comprometer su integridad (es decir, precisión y confiabilidad), para influir en la toma de decisiones, reducir la confianza en los sistemas o causar efectos físicos adversos […]. Los agentes cibernéticos rusos, que publican desinformación en páginas web comerciales, podrían tratar de alterar los medios en línea como una forma para influir en el discurso público y crear confusión. La doctrina militar china describe el uso de las operaciones de engaño cibernético para ocultar intenciones, modificar datos almacenados, transmitir datos falsos, manipular el flujo de información o influir en los sentimientos públicos, todo ello para inducir errores y fallos de cálculo en la toma de decisiones.[28]

También estamos preocupados por los criminales. Entre 2014 y 2016, el Departamento del Tesoro de Estados Unidos realizó una serie de ejercicios para ayudar a los bancos a planificar ataques de manipulación de datos relacionados con transacciones y comercios,[29] y luego creó un programa para ayudarlos a restablecer las cuentas de los clientes tras un ataque generalizado.[30] Alguien que inserte datos falsos en el sistema financiero podría causar estragos, ya que nadie sabría qué transacciones son reales, y ordenarlas de forma manual podría llevar semanas.

Todo esto hace que la seguridad sea crítica de una manera que no lo había

sido antes. Hay una diferencia fundamental entre bloquear tu ordenador y perder los datos de tu hoja de cálculo, y romper tu marcapasos y perder la vida, aunque sean los mismos chips de ordenador, el mismo sistema operativo, el mismo software, la misma vulnerabilidad y el mismo programa de ataque.

LOS ALGORITMOS SE ESTÁN VOLVIENDO AUTÓNOMOS Y MÁS PODEROSOS

En su núcleo, los ordenadores ejecutan algoritmos de software. En el capítulo 1 hablamos sobre errores, vulnerabilidades y el aumento de la vulnerabilidad debido a la complejidad, pero hay un nuevo aspecto que empeora el problema.

El aprendizaje automático es una clase particular de algoritmo de software. Básicamente, es una forma de instruir a un ordenador para que aprenda, alimentándolo con una enorme cantidad de datos y diciéndole cuándo lo está haciendo bien o mal. El algoritmo de aprendizaje de máquinas se modifica para su mejora con mayor frecuencia.[31]

Los algoritmos de aprendizaje automático están apareciendo en todas partes porque hacen las cosas más rápido y mejor que los humanos, en especial cuando se trata de grandes cantidades de datos. Nos dan los resultados de nuestra búsqueda, comprueban qué hay en las noticias de nuestra red social, califican nuestra solvencia crediticia, determinan para qué servicios gubernamentales somos elegibles y nos recomiendan libros y películas que nos gusten según lo que ya hemos leído o visto. Además, clasifican las fotografías y traducen el texto de un idioma a otro;[32] juegan al Go tan bien como un maestro;[33] leen radiografías y diagnostican cánceres; [34] informan sobre las decisiones de libertad bajo fianza, sentencia y libertad condicional;[35] analizan el habla para evaluar el riesgo de suicidio[36] y los rostros para prever la homosexualidad,[37] y también son mejores que nosotros determinando la calidad del buen vino de Burdeos,[38] contratando obreros[39] y decidiendo si apostar o no en el fútbol.[40] El aprendizaje automático se utiliza para detectar correos electrónicos no deseados o de phishing, además de para hacer que estos últimos sean más personalizados y creíbles, y por lo tanto más efectivos.[41]

Debido a que estos algoritmos se programan en esencia a sí mismos, puede ser imposible para los humanos entender lo que hacen. Por ejemplo, Deep Patient es un sistema de aprendizaje automático que tiene un éxito

sorprendente en la predicción de la esquizofrenia, la diabetes y algunos tipos de cáncer; en muchos casos, sus resultados son mejores que los de los humanos expertos.[42] Pero, aunque el sistema funcione, nadie sabe cómo lo hace, incluso después de analizar el algoritmo de aprendizaje automático y sus resultados.[43]

En general nos gusta esto. Preferimos el sistema de diagnóstico de aprendizaje automático más preciso por encima del técnico humano, aunque no pueda explicarse por sí mismo. Por esta razón, los sistemas de aprendizaje automático están cada vez más generalizados en muchas áreas de la sociedad.

Por las mismas razones permitimos que los algoritmos tengan mayor autonomía, que es la capacidad de los sistemas para actuar de forma independiente, sin supervisión ni control humano. Los sistemas autónomos pronto estarán en todas partes. Un libro de 2014, *Autonomous Technologies* (*Tecnologías autónomas*), contiene capítulos sobre vehículos para la agricultura, aplicaciones de paisajismo y monitores ambientales, y todos ellos funcionan con autonomía.[44] Los automóviles ahora tienen características autónomas, como permanecer dentro de los carriles, seguir a una distancia fija detrás de otro automóvil y frenar sin intervención humana para evitar colisiones. También son autónomos los agentes de software: programas que hacen cosas en tu nombre, como comprar acciones si el precio cae por debajo de cierto punto.

Estamos permitiendo, además, que los algoritmos tengan una entidad física. En esto estaba pensando cuando describí Internet+ como un Internet que puede afectar al mundo de una manera física directa. Cuando miras a tu alrededor, los ordenadores con entidad física están por todas partes, desde dispositivos médicos integrados hasta automóviles y plantas de energía nuclear.

Algunos algoritmos que podrían no parecer autónomos en realidad sí lo son. Si bien es cierto que son los jueces quienes toman decisiones referentes a la libertad bajo fianza, si estos hacen lo que recomienda el algoritmo porque creen que está menos sesgado, entonces el algoritmo es igual de bueno por sí solo. De igual manera, si un médico nunca contradice un algoritmo que toma decisiones sobre la cirugía del cáncer, posiblemente por temor a una demanda por negligencia profesional, o si un oficial del ejército nunca contradice a un algoritmo que decide dónde dirigirse en un ataque con un dron, esos algoritmos son igual de buenos por sí solos. Añadir a un humano a la ecuación no cuenta a menos que sea él quien decida en realidad.

Los riesgos en todos estos casos son considerables.

Los algoritmos pueden hackearse, ya que se ejecutan utilizando un software y, como decía en el capítulo 1, el software también puede piratearse. Todos los ejemplos de los capítulos anteriores son el resultado de softwares hackeados.

Los algoritmos requieren entradas precisas; necesitan información, a menudo sobre el mundo real, para funcionar bien, así que debemos asegurarnos de que los datos estén disponibles cuando los algoritmos los necesiten y de que sean correctos, ya que a veces están sesgados de forma natural, por lo que una de las formas de atacar los algoritmos es manipulando los datos introducidos. Básicamente, si dejamos que los ordenadores piensen por nosotros y los datos de entrada subyacentes están alterados, entonces harán mal los cálculos y es posible que nunca lo sepamos.

En situaciones de lo que se denomina aprendizaje automático adverso, el atacante intenta descubrir cómo alimentar al sistema con datos específicos que hagan que falle de una manera concreta. Un proyecto de investigación se centró en los algoritmos de clasificación de imágenes y descubrió que eran capaces de crear imágenes irreconocibles para los humanos y aun así las redes de aprendizaje automático las clasificaban con mucha fiabilidad.[45] Un proyecto de investigación relacionado fue capaz de engañar a los sensores visuales de los automóviles con señales de tráfico falsas de una manera que no engañaría a los ojos ni al cerebro humanos.[46] Otro proyecto engañó a un algoritmo, sin saber nada sobre su diseño, para clasificar los rifles como helicópteros.[47] (Ahora este es un ejercicio habitual en las clases universitarias de informática: engañar al clasificador de imágenes).

De la misma manera que el robot Tay de Microsoft con el que podías chatear se volvió racista y misógino debido a los datos introducidos a propósito,[48] los hackers pueden entrenar todo tipo de algoritmos de aprendizaje automático para que hagan cosas inesperadas. Los spammers también podrían descubrir cómo engañar a los algoritmos de aprendizaje automático antispam. Cuanto más comunes y poderosos se vuelven los algoritmos de las máquinas, más ataques de este tipo cabría esperar.

También hay nuevos riesgos en la velocidad de los algoritmos. Los ordenadores toman decisiones y hacen las cosas mucho más rápido que las personas: pueden realizar operaciones con acciones de la bolsa en milisegundos o apagar el suministro eléctrico de millones de hogares al mismo tiempo. Los algoritmos pueden replicarse repetidamente en diferentes ordenadores, y cada implementación toma millones de decisiones por segundo. Por un lado, esto es genial porque los algoritmos pueden escalarse

de formas imposibles para las personas, al menos de una manera fácil, económica y consistente; por otro, la velocidad también puede hacer que sea más difícil realizar verificaciones significativas del comportamiento algorítmico.

A menudo lo único que ralentiza los algoritmos es su interacción con personas. Cuando interactúan entre sí a una velocidad algorítmica, los resultados combinados pueden escapar de todo control. Lo que hace que un sistema autónomo sea más peligroso es que puede causar un daño grave antes de que un humano intervenga.

En 2017, Dow Jones publicó por error una historia sobre la compra de Apple por Google.[49] Obviamente, era un bulo, y cualquier persona que lo leyera lo habría comprendido de inmediato, pero los robots de comercio bursátil fueron engañados y eso influyó en los precios de las acciones durante dos minutos hasta que la historia se desmintió.

Este fue solo un problema menor. En 2010, hubo un gran desplome repentino de acciones (*flash crash*) en la bolsa estadounidense. En cuestión de minutos, una interacción fortuita causó la pérdida de un billón de dólares de valor en el mercado bursátil y el incidente terminó con la quiebra de la empresa que originó el problema.[50] En 2013, los hackers irrumpieron en la cuenta de Twitter de Associated Press y anunciaron un ataque falso a la Casa Blanca, lo que hizo que los mercados de valores cayeran un 1 % en segundos.[51]

También deberíamos esperar que los atacantes utilicen sistemas autónomos de aprendizaje automático para inventar nuevas técnicas de ataque, conseguir datos personales con fines fraudulentos o elaborar correos electrónicos de phishing más creíbles.[52]

En la conferencia DefCon de 2016, la Agencia de Proyectos de Investigación Avanzada de Defensa de Estados Unidos (DARPA, por sus siglas en inglés) patrocinó un nuevo tipo de concurso de piratería. Capturar la bandera es un deporte popular de piratería: los organizadores crean una red llena de errores y vulnerabilidades, y los equipos defienden su propia parte de la red mientras atacan las partes de otros equipos. El Cyber Grand Challenge fue similar, excepto porque los equipos enviaron programas que intentaron hacer lo mismo automáticamente.[53] Los resultados fueron impresionantes. Un programa encontró una vulnerabilidad no detectada antes en la red, la parcheó y luego procedió a explotarla para atacar a otros equipos.[54] En un concurso posterior, que contó con equipos tanto humanos como informáticos, las máquinas superaron a los humanos.[55]

Estos algoritmos serán cada vez más sofisticados y más capaces. Los atacantes usarán software para analizar las defensas y desarrollar nuevas técnicas de ataque.[56] La mayoría de los expertos en seguridad esperan que el software ofensivo de ataque autónomo sea común en un futuro cercano.[57] Luego solo será cuestión de mejorar la tecnología y esperar a que los atacantes informáticos mejoren a un ritmo mucho más rápido que los humanos; en otros cinco años, los programas autónomos podrían vencer rutinariamente a todos los equipos humanos.

Mike Rogers, alto cargo del Comando Cibernético de Estados Unidos y director de la NSA, decía lo siguiente en 2016: «La inteligencia artificial y el aprendizaje automático […] son fundamentales para el futuro de la ciberseguridad […]. Tenemos que encontrar nuestro camino y ver cómo vamos a lidiar con todo esto. Para mí, no es una cuestión de si va a ocurrir, sino cuándo».[58]

Los robots son el ejemplo más sugerente de autonomía de software combinada con agente físico. Los investigadores ya han explotado vulnerabilidades en robots para tomar su control de forma remota[59] y han encontrado vulnerabilidades en los robots quirúrgicos teleoperados[60] e industriales.[61]

Mención especial merecen los sistemas militares autónomos.[62] El Departamento de Defensa de Estados Unidos define un arma autónoma como aquella que selecciona un objetivo y dispara sin la intervención de un operador humano.[63] Todos los sistemas de armas son letales y todos son propensos a los accidentes. Incorporar autonomía aumenta significativamente el riesgo de muerte accidental. Si las armas se computarizan (antes de que sean verdaderos soldados robot), también serán vulnerables a la piratería. Las armas pueden desactivarse o funcionar mal y, si son autónomas, podría piratearse un gran número de ellas para enfrentarlas entre sí o con sus aliados humanos.[64] Además, aquellas que no puedan retirarse o desactivarse, y que también operen a velocidades de ordenador, podrían causar todo tipo de problemas letales para amigos y enemigos por igual.

Todo esto converge en la inteligencia artificial. En los últimos años hemos leído algunas predicciones sobre los peligros de la IA. Los tecnólogos Bill Gates, Elon Musk y Stephen Hawking, así como el filósofo Nick Bostrom, han advertido sobre un futuro en el que la inteligencia artificial (ya sean robots o algo menos personificado) se vuelva tan poderosa que se adueñe del mundo y esclavice, extermine o ignore a la humanidad.[65] Los riesgos

podrían ser remotos, argumentan, pero son tan serios que sería ridículo ignorarlos.[66]

No me preocupa demasiado la IA; considero que tenerle miedo es más un espejo de nuestra propia sociedad que un presagio del futuro.[67] La inteligencia artificial y la robótica inteligente son la culminación de varias tecnologías precursoras, como los algoritmos de aprendizaje automático, la automatización y la autonomía. Los riesgos de seguridad de esas tecnologías predecesoras ya están con nosotros y aumentan a medida que las tecnologías se vuelven más poderosas y más comunes. Así que, si bien me preocupan los vehículos inteligentes y los que no tienen conductor, la mayoría de los riesgos ya son habituales en los que tienen conductor y están conectados a Internet. Y aunque estoy preocupado por los soldados robot, la mayoría de los riesgos ya existen en los sistemas de armas autónomas.

Además, como ya señaló el especialista en robótica Rodney Brooks, «mucho antes de que surjan esas máquinas, surgirán otras algo menos inteligentes y beligerantes. Antes de eso habrá máquinas realmente gruñonas. Antes de eso habrá máquinas bastante molestas. Y antes, arrogantes y desagradables máquinas».[68] Creo que veremos nuevos riesgos de seguridad mucho antes de que ellas lleguen.

NUESTRAS CADENAS DE SUMINISTRO SON CADA VEZ MÁS VULNERABLES

Hay otra clase de ataques que hemos abordado solo de forma secundaria: los ataques a la cadena de suministro. Se dirigen a la producción, distribución y mantenimiento de ordenadores, software, equipos de redes, etc.; es decir, todo lo que comprende Internet+, o sea, todo.

Por ejemplo, existe la sospecha generalizada de que los productos de conexión de redes fabricados por la compañía china Huawei contienen puertas traseras controladas por el Gobierno[69] y que los productos de seguridad informática de los laboratorios Kaspersky están comprometidos por el Gobierno ruso.[70] En 2018, los funcionarios de inteligencia estadounidenses desaconsejaron la compra de teléfonos inteligentes de las compañías chinas Huawei y ZTE.[71] En 1997, la compañía israelí Check Point fue perseguida por los rumores de que el Gobierno del país había añadido puertas traseras a sus productos.[72] En Estados Unidos, la NSA instaló en secreto un equipo de escuchas ilegales en las instalaciones de AT&T y recopiló información sobre las llamadas telefónicas de los

proveedores móviles.[73] Todos estos pirateos se dirigen contra los productos y servicios básicos que utilizamos en Internet y minan la confianza que tenemos en ellos, y demostraron la vulnerabilidad de nuestra cadena de suministro de productos tecnológicos.[74]

Estos riesgos nunca se consideraron en el curso de la evolución de Internet y son en gran medida un resultado accidental de su inesperado crecimiento y éxito. Nuestro hardware está hecho en Asia, donde los costes de producción son bajos; nuestros programadores provienen de todo el mundo y cada vez se fabrican más programas en países como India y Filipinas, donde la mano de obra cuesta menos que en Estados Unidos. El resultado es un lío en la cadena de suministro. Los chips de ordenador de un producto pueden fabricarse en un país y ensamblarse en otro, ejecutar software escrito en un tercero e integrarse en un sistema final en un cuarto antes de que se evalúe su calidad en un quinto y se venda a un cliente en un sexto. En cualquiera de esos pasos, los participantes en la cadena de suministro pueden alterar la seguridad del sistema final. En todos esos países los Gobiernos locales tienen sus propios intereses, y cualquiera de ellos puede obligar a los ciudadanos a cumplir sus órdenes. Añadir una puerta trasera a un chip de ordenador durante el proceso de fabricación es sencillo y resistente a la mayoría de las técnicas de detección.[75]

Una de las formas que tienen los Gobiernos para defenderse de algunos de estos ataques es exigir que les enseñen el código fuente del software que compran. China exige ver el código fuente,[76] igual que hace Estados Unidos.[77] Kaspersky se ofreció a permitir que cualquier Gobierno viera su código fuente después de que lo acusaran de tener puertas traseras insertadas por el Gobierno ruso.[78] Por supuesto, esto es un arma de doble filo: los países pueden usar el código fuente ofrecido para encontrar vulnerabilidades que explotar. En 2017, HP Enterprise se enfrentó a críticas porque le dio a Rusia el código fuente de su línea ArcSight de productos de seguridad de red.[79]

Los Gobiernos no solo están comprometiendo los productos y servicios en sus propios países durante el proceso de diseño y producción, sino también impidiendo el proceso de distribución, ya sea de forma individual o masiva. Según los documentos de la NSA de Edward Snowden, este organismo buscaba incluir su propia puerta trasera en el equipo de Huawei.[80] También sabemos por los documentos de Snowden que los empleados de la NSA interceptaban de manera rutinaria los equipos de redes Cisco que la empresa enviaba a sus clientes extranjeros e instalaban en ellos material de espionaje.[81] Esto se hizo sin el conocimiento de Cisco (y la compañía estaba furiosa

cuando lo descubrió),[82] pero estoy seguro de que hay otras compañías estadounidenses más cooperativas. Se han descubierto puertas traseras en los cortafuegos Juniper[83] y en los rúters D-Link[84], aunque no sabemos quién las instaló.

Los hackers han introducido aplicaciones falsas en la tienda de Google Play: parecen aplicaciones reales y actúan como tal (y tienen nombres parecidos para engañar a las personas), pero recopilan información personal con fines maliciosos. Un informe decía que 4,2 millones de aplicaciones falsas fueron descargadas por personas confiadas en 2017;[85] entre ellas se incluía una que imitaba a WhatsApp,[86] aunque los usuarios tuvieron suerte, ya que tan solo se había diseñado para robar ingresos de publicidad, no para escuchar las conversaciones de las personas.

Aquí hay otros ejemplos más de 2017: piratas informáticos vinculados con China pusieron en peligro la web real de una popular herramienta de Windows llamada CCleaner, lo que provocó que millones de usuarios descargaran una versión del software infectada con malware;[87] unos piratas informáticos desconocidos dañaron el mecanismo auténtico de actualización para que un software de contabilidad ucraniano difundiera el malware NotPetya en todo el país;[88] otro grupo utilizó actualizaciones antivirus falsas para propagar malware;[89] algunos investigadores demostraron cómo hackear un iPhone infectando una pantalla de reemplazo hecha por terceros,[90] y hay suficientes ataques similares como para que algunas personas estén advirtiendo de que no debe comprarse ningún dispositivo IoT usado de sitios como eBay.[91]

Los sistemas más grandes también son vulnerables a estos ataques. En 2012, compañías chinas, financiadas por su país, construyeron la nueva sede de la Unión Africana en Adís Abeba (Etiopía), con los sistemas de telecomunicaciones del edificio incluidos, pero en 2018, la Unión Africana descubrió que China estaba usando esa infraestructura para espiar los ordenadores de la organización.[92] Esto me recuerda a la embajada de Estados Unidos construida en Moscú por contratistas rusos durante la Guerra Fría: estaba plagada de dispositivos de escucha.[93]

Las vulnerabilidades de la cadena de suministro son un enorme problema de seguridad que estamos ignorando en gran medida. El comercio es tan global que no es factible para ningún país mantener toda su cadena de suministro dentro de sus fronteras. Casi todas las compañías de tecnología de Estados Unidos fabrican su hardware en países como Malasia, Indonesia, China y Taiwán. Y, si bien el Gobierno de Estados Unidos a veces aborda

este problema bloqueando fusiones o adquisiciones puntuales, o prohibiendo cierto hardware o productos de software, son solo intervenciones menores en un problema mucho más grande.

SOLO ESTÁ EMPEORANDO

Nuestra dependencia de Internet se está volviendo crítica. En un discurso de 2012, el secretario de Defensa Leon Panetta advirtió de lo siguiente:

> Una nación agresora o un grupo extremista podría usar este tipo de herramientas cibernéticas para obtener el control de los interruptores críticos. Podrían descarrilar trenes de pasajeros o, incluso más peligroso, descarrilar trenes cargados con productos químicos letales. Podrían contaminar el suministro de agua en las principales ciudades o apagar la red eléctrica en grandes zonas del país.[94]

Esto es de la *Evaluación de amenazas mundial* de 2017:

> Las amenazas cibernéticas también representan un riesgo creciente para la salud pública, la seguridad y la prosperidad, ya que las tecnologías cibernéticas se integran con la infraestructura crítica en sectores clave. Estas amenazas se amplifican con nuestra manera constante de delegar los roles de toma de decisiones, detección y autenticación en sistemas automatizados potencialmente vulnerables.[95]

Esto es de la versión de 2018:

> El potencial de sorpresa en el ámbito cibernético aumentará en el próximo año y más allá a medida que miles de millones más de dispositivos digitales estén conectados (con relativamente poca seguridad incorporada), y tanto los Estados nación como los agentes malignos se vuelvan más avezados y mejor equipados para el uso de cada vez más kits de herramientas cibernéticas de todo tipo. Aumenta el riesgo de que algunos adversarios realicen ataques cibernéticos (como la eliminación de datos o interrupciones localizadas y temporales de infraestructura crítica) contra Estados Unidos en una crisis parecida a una guerra.[96]

Sin duda algo de esto es una exageración, pero mucho no lo es.

En 2015, Lloyd's of London desarrolló el escenario hipotético de un ataque cibernético a gran escala en la red eléctrica de Estados Unidos.[97] El escenario de ataque fue realista, no más sofisticado que lo que Rusia le hizo a Ucrania en diciembre de 2015 y junio de 2017, combinado con el ataque de demostración del Laboratorio Nacional de Idaho contra generadores de energía. Los investigadores de Lloyds imaginaron un apagón que afectara a 95 millones de personas en quince estados y que durara desde veinticuatro horas hasta varias semanas, con un coste de entre 250.000 millones y 1 billón de dólares, dependiendo de los detalles del escenario.

El título de este libro, un auténtico cebo para los amantes del mundo digital, hace referencia al escenario de ciencia ficción de un mundo tan interconectado, con ordenadores y redes tan integrados en nuestras infraestructuras técnicas más importantes, que alguien podría potencialmente destruir la civilización con unos pocos clics del ratón. No estamos cerca de ese futuro, y no tengo claro que alguna vez lo estemos, pero los riesgos se incrementan de manera catastrófica.

Hay un principio general en marcha. Los avances tecnológicos permiten ampliar los ataques y una mejor tecnología significa que menos atacantes pueden hacer más daño. Alguien con una pistola puede dañar más que alguien con una espada, y esa misma persona armada con una ametralladora, todavía más.[98] Si vas armado con explosivos plásticos puedes hacer más daño que con dinamita, y si tienes un misil nuclear, el daño será todavía mayor. Un dron armado será más barato y más sencillo de fabricar; quizá algún día sea posible hacer uno fácilmente con una impresora 3D (hay una demostración chapucera en YouTube).[99]

Ya hemos visto esta escalada en Internet. Los delincuentes cibernéticos pueden robar cantidades mayores de dinero de más cuentas bancarias y con más rapidez que los delincuentes a pie; los piratas digitales pueden copiar más películas más deprisa y colgarlas en los servidores en la nube que cuando había que usar cintas VHS, y los Gobiernos del mundo han aprendido que Internet les permite escuchar más eficientemente que las antiguas redes telefónicas. Internet facilita que los ataques se amplíen en un grado imposible de imaginar sin ordenadores y redes.

¿Recuerdas el capítulo 1, donde hablábamos sobre que la distancia no importa, las roturas de clase y la capacidad de incluir habilidades en un software? Estas tendencias son aún más peligrosas conforme nuestros sistemas informáticos se vuelven más críticos para nuestras infraestructuras. Los riesgos incluyen que alguien estrelle *todos* los coches (para ser justos,

sería más factible hacerlo con una marca y año de un modelo en particular con el mismo software) o que cierren *todas* las plantas de energía, que roben *todos* los bancos a la vez o que alguien cometa un asesinato en masa al tomar el control de *todas* las bombas de insulina del mismo fabricante. Estos riesgos catastróficos no eran posibles antes de la interconexión, la automatización y la autonomía que ofrece Internet.

Cuanto más nos adentremos en el mundo de Internet+, donde los ordenadores impregnan nuestras vidas a todos los niveles, más peligrosas serán las roturas de clase. La combinación de la automatización y el accionamiento a distancia dará a los atacantes más poder e influencia que nunca. Estados Unidos siempre se ha visto a sí mismo como una sociedad que se arriesga, y preferimos actuar primero y limpiar después. Pero, si los riesgos son demasiado altos, ¿podemos seguir en esa línea?

El riesgo que me mantiene despierto por la noche no es un Pearl Harbor cibernético, donde una nación lanza un ataque sorpresa contra otra, sino un ataque criminal en aumento fuera de control.

Además, existe una asimetría entre los diferentes países. Las democracias liberales son más vulnerables que los países totalitarios, en parte porque confiamos más en Internet+ y para cosas más críticas, y en parte porque no estamos involucrados en un control centralizado de mano dura.[100] En una conferencia de prensa de 2016, el presidente Obama admitió lo siguiente: «Nuestra economía está más digitalizada, es más vulnerable, en parte porque […] tenemos una sociedad más abierta y participamos en menos en el control y la censura de lo que sucede en Internet».[101]

Esta asimetría complica la disuasión,[102] hace más difícil prevenir la escalada y nos sitúa en una posición más peligrosa con respecto a otros países del mundo.

Algo interesante sucede cuando atacantes cada vez más poderosos interactúan con la sociedad. Conforme la tecnología hace que estos sean más poderosos, el número de ellos que somos capaces de tolerar disminuye. Piensa en esto como si fuera un juego de números. Gracias a la forma en que nos comportamos los humanos como especie y como comunidad, cada sociedad tendrá cierto porcentaje de individuos malos, lo que significa un determinado índice de criminalidad. Al mismo tiempo, existe una tasa de criminalidad particular que la sociedad está dispuesta a soportar; a medida que aumenta la efectividad de cada criminal, el número total de delincuentes que una sociedad puede admitir disminuye.

A modo de experimento mental, supón que un ladrón común puede robar una casa por semana, y una ciudad de cien mil viviendas estaría dispuesta a vivir con una tasa de robos del 1 %, lo que significa que la ciudad puede tolerar veinte ladrones. Pero, si la tecnología aumenta repentinamente la eficiencia de cada ladrón para que pueda robar cinco casas a la semana, la ciudad entonces solo podrá tolerar a cuatro ladrones; por tanto, tendrá que detener a los otros dieciséis para poder mantener la misma tasa de robo del 1 %.

La sociedad hace esto en realidad. La gente no calcula la ecuación de manera explícita, pero eso no lo hace menos cierto. Si la tasa de criminalidad es demasiado alta, nos quejamos de que no hay suficientes policías; si es demasiado baja, nos quejamos de que estamos gastando demasiado dinero en policía. En el pasado, con criminales ineficientes, estábamos dispuestos a vivir con un porcentaje determinado de criminales dentro de nuestra sociedad; sin embargo, a medida que la tecnología hace que cada criminal individual sea más eficiente, el porcentaje que podemos tolerar disminuye.

Este es el verdadero riesgo del terrorismo en el futuro. Debido a que los terroristas podrían causar mucho más daño con la tecnología moderna, tenemos que asegurarnos de que haya proporcionalmente menos. Por eso se ha hablado tanto de terroristas con armas de destrucción masiva. Las tecnologías a las que más temíamos después del 11S eran nucleares, químicas y biológicas.[103] Más tarde, se añadieron armas radiológicas a la lista. Las armas cibernéticas se han situado en el mismo rango que las otras, sobre todo por la gran incertidumbre sobre lo nefastas que pueden ser.[104] Las armas de pulsos electromagnéticos están diseñadas específicamente para desactivar los sistemas electrónicos.[105] Estoy seguro de que los avances tecnológicos futuros darán como resultado tecnologías de destrucción masiva todavía inimaginadas, pero estas son las que tememos hoy.[106]

El terrorismo en Internet está a unos pocos años de aparecer. Incluso la *Evaluación mundial de amenazas* de 2017 limita las preocupaciones sobre el terrorismo e Internet a la coordinación y el control:

> Los terroristas —incluyendo el Estado Islámico de Irak y ash-Sham (ISIS)— también continuarán utilizando Internet para organizar, reclutar, difundir propaganda, recaudar fondos, recopilar información, inspirar acciones a sus seguidores y coordinar operaciones. Hizbulá y Hamás seguirán con sus progresos cibernéticos dentro y fuera de Oriente Medio. ISIS continuará buscando oportunidades para encontrar y divulgar información confidencial sobre los ciudadanos de Estados

> Unidos, parecidas a sus operaciones de 2015, que divulgaron información sobre el personal militar de Estados Unidos tratando de inspirar ataques.[107]

Mi suposición es que no veremos el terrorismo de Internet hasta que pueda matar gente de manera gráfica. Apagar la electricidad de un millón de personas no aterroriza de la misma manera; ocurre por accidente con frecuencia, e incluso aunque algunas personas mueren, solo ocupará una nota a pie de página. Conducir un camión hacia una multitud de personas garantiza el primer puesto en las noticias de la noche, incluso aunque sea de bajo nivel tecnológico. Pero los atacantes de Internet están volviéndose más agresivos, ingeniosos y tenaces cada año, y algún día el terrorismo de la Red que involucre aviones o automóviles será posible.

Lo que hace que estos ataques sean tan diferentes de los convencionales es el daño que pueden causar. Las consecuencias posibles son tan grandes que creemos que no podremos permitirnos tener ni siquiera un incidente grave. Volviendo al experimento mental: tememos que los avances tecnológicos hagan que cada atacante sea tan poderoso que no podamos tolerar ni un solo ataque exitoso.

En noviembre de 2001, el entonces vicepresidente Richard Cheney formuló la doctrina del uno por ciento, descrita por el periodista Ron Suskind: «Si hubiera incluso un uno por ciento de probabilidades de que los terroristas obtuvieran un arma de destrucción masiva, y ha habido una pequeña probabilidad de ese tipo durante algún tiempo, Estados Unidos debería actuar entonces como si fueran una certeza».[108] En esencia, acabo de proporcionar una justificación para la doctrina de Cheney.

Algunos de estos nuevos riesgos no tienen nada que ver con los ataques de países hostiles o terroristas; más bien surgen de la naturaleza misma de Internet+, que abarca y conecta casi todo haciéndolo vulnerable *al mismo tiempo*. Igual que las grandes empresas de servicios públicos y los sistemas financieros, Internet+ es un sistema demasiado grande para fallar, o al menos la seguridad es muy importante: no puede fallar, porque los atacantes son lo bastante poderosos para tener éxito y sus resultados serían demasiado catastróficos como para considerarlos.

Estos errores podrían provenir de ataques más pequeños, o incluso de accidentes que se salen de madre. Durante mucho tiempo pensé que el apagón de 2003 que sufrió la mayor parte del noreste de Estados Unidos y el sureste de Canadá fue el resultado de un ataque cibernético.[109] No fue deliberado de ninguna manera, pero ocurrió el día en que un gusano de Windows, Blaster,

estaba propagándose de forma virulenta y hacía que los ordenadores se bloquearan.[110] El informe oficial sobre el apagón concretó que ninguno de los ordenadores que controlaban directamente la red eléctrica ejecutaba Windows, pero sí los que monitorizaban a esos otros ordenadores, y el informe dijo que algunos de ellos estaban apagados.[111] Culpo al virus por ocultar el pequeño apagón inicial lo suficiente como para que tuviera efectos catastróficos, si bien los creadores del virus no tenían ni idea de que esto sucedería y no podrían haberlo hecho a propósito.

De modo similar, los autores de la botnet Mirai no se dieron cuenta de que su ataque contra Dyn provocaría que todas aquellas páginas web populares quedaran sin conexión.[112] No creo que supieran siquiera qué compañías usaban los servicios de DNS de Dyn, ni que había un único punto de error sin respaldo alguno. De hecho, fueron tres estudiantes universitarios quienes escribieron la botnet para conseguir ventaja en el juego Minecraft.[113]

El daño a los ordenadores que controlan los sistemas físicos se expande hacia fuera. Un ataque de 2012 contra la compañía petrolera nacional de Arabia Saudí solo afectó a la red de TI de la compañía, pero borró todos los datos de más de treinta mil discos duros, lo que paralizó la compañía durante semanas y afectó a la producción de petróleo durante meses, con repercusiones en la disponibilidad global.[114] El gigante naviero Maersk estuvo tan afectado por NotPetya que tuvo que detener las operaciones en 76 terminales portuarias de todo el mundo.[115]

Los dispositivos que por lo general no están asociados a la infraestructura crítica también pueden causar catástrofes. Ya mencioné las rupturas de clase de sistemas, automóviles —sobre todo coches sin conductor— y dispositivos médicos. A esto podemos añadir asesinatos en masa por enjambres de drones armados,[116] la interrupción de sistemas críticos por botnets cada vez más masivas, el uso de impresoras biológicas para producir patógenos letales, IA maliciosas que esclavizan a la humanidad, códigos dañinos recibidos de extraterrestres que hackean el planeta[117] y todas esas cosas en las que aún no hemos pensado.[118]

Bueno, hagamos una pausa para recuperar el aliento. Tendemos a sentir un pánico indebido por el futuro. Piensa en todos los escenarios del fin del mundo a lo largo de la historia que nunca sucedieron. Durante la Guerra Fría, muchos estaban seguros de que los humanos se matarían en una guerra termonuclear, por lo que decidieron ahorrar menos dinero a largo plazo[119] y otros decidieron no tener hijos, porque ¿cuál era el sentido?[120] En retrospectiva existen muchas razones por las que ni Estados Unidos ni la

URSS comenzaron la tercera guerra mundial, pero ninguna de ellas era obvia en ese momento. En parte, resultó que los líderes de nuestro mundo no eran tan fanáticos como pensábamos. A lo largo de los años hubo muchos fallos técnicos tanto en los sistemas de detección de misiles de Estados Unidos como en los de la URSS, situaciones en las que los equipos mostraron claramente que el país estaba bajo un ataque nuclear, y en ningún caso tomaron represalias.[121] La crisis de los misiles en Cuba es quizá lo más cerca que estuvimos políticamente de una guerra nuclear,[122] aunque la falsa alarma de 1983 tiene un merecido segundo lugar;[123] sin embargo, no sucedió.

Nuestros temores colectivos después de los atentados terroristas del 11 de septiembre fueron parecidos. Ese acontecimiento singular, con un número de muertos de tres mil personas y un coste de 10.000 millones de dólares en daños a la propiedad y la infraestructura, fue muy desproporcionado en comparación con el resto de los ataques terroristas que hemos experimentado en la historia de nuestro planeta (si bien fue mucho menos dañino que el número anual de muertes por automóviles, enfermedades del corazón o malaria).[124] Pero, en lugar de considerarlo como un hecho singular que probablemente no se repita pronto, la gente decidió que sería lo habitual.[125] La verdad es que el ataque terrorista típico se parece más a los atentados de la maratón de Boston: tres personas muertas, 264 heridas y no demasiados daños derivados.[126] En conjunto, las bañeras, los electrodomésticos y los ciervos matan a muchos más estadounidenses cada año en promedio que los terroristas.[127] Pero, aunque parezca que estamos saliendo de nuestro trastorno colectivo de estrés postraumático al 11S, todavía tenemos mucho más miedo a las amenazas terroristas de lo que tiene sentido según el riesgo real.[128] En general, las personas somos muy malas evaluando riesgos.[129]

Durante años he estado escribiendo sobre lo que yo llamo *amenazas de argumento de película*: amenazas de seguridad tan extravagantes que, si bien serían excelentes tramas para películas, es tan poco probable que sucedan que no debemos perder el tiempo preocupándonos por ellas. Acuñé el término en 2005 para burlarme de todas las historias terroríficas y demasiado específicas sobre terrorismo que los medios de comunicación nos estaban vendiendo: terroristas con equipo de buceo, que dispersan ántrax por los cultivos o que contaminan el suministro de leche.[130] Mi argumento tenía dos caras: una es que somos una especie de narradores de historias, y las historias detalladas evocan un temor en nosotros que las discusiones generales sobre el terrorismo no alcanzan,[131] y la otra, que no tiene sentido defenderse contra tramas

específicas, sino que en su lugar deberíamos centrarnos más en medidas de seguridad generales que funcionen contra cualquiera de ellas.[132] En lo que respecta al terrorismo, eso sería inteligencia, investigación y respuesta de emergencia. Las medidas de seguridad inteligentes serán diferentes para otras amenazas.

Es fácil descartar los escenarios más extremos en este capítulo como amenazas de película. Es probable que algunos de ellos lo sean de manera individual, pero colectivamente son la clase de amenazas que tienen precursores en el pasado y que se volverán más comunes en el futuro. Algunos de ellos están sucediendo ahora, con una frecuencia variable. Y aunque tal vez me equivoque en los pormenores, las líneas generales son correctas. De la misma forma que con la lucha contra el terrorismo, nuestro objetivo no es empezar a cortar cabezas y detener algunas amenazas particularmente importantes, sino diseñar sistemas que desde el principio tengan menos probabilidades de recibir ataques fructíferos.

SEGUNDA PARTE
LAS SOLUCIONES

LA SEGURIDAD DE Internet+ parece bastante desoladora. Las amenazas aumentan, los atacantes son más descarados y las defensas cada vez más inadecuadas.

Toda la culpa no debería recaer en la tecnología. Los ingenieros ya saben cómo solucionar algunos de los problemas que he mencionado. Cientos de empresas, e incluso más investigadores académicos, están trabajando en nuevas y mejores tecnologías de seguridad contra las amenazas emergentes. Los desafíos son difíciles, pero son de una dificultad similar a la de enviar a un hombre a la luna, no de viajar más rápido que la luz. Y, si bien nada es la panacea, en realidad no hay ningún límite a la creatividad de los ingenieros que quieran encontrar soluciones novedosas para problemas difíciles.

Aun así, no creo que nada de esto vaya a mejorar pronto. Mi pesimismo proviene principalmente de los desafíos de las políticas. El estado actual de la seguridad de Internet es resultado directo de las decisiones comerciales de empresas y de las decisiones militares o de espionaje tomadas por los Gobiernos; todo lo mencionado en el capítulo 4. Lo que hemos aprendido de las últimas décadas es que la seguridad informática es más un problema humano que técnico. Lo importante es la ley y la economía, la psicología y la sociología, y lo crítico es la política y el Gobierno.

Piensa en el spam. Durante años era un problema con el que tenías que lidiar en tu ordenador, o tal vez tu proveedor de servicios de Internet proporcionaba servicios locales contra el correo no deseado. La forma más eficiente de identificar y eliminar el spam era en la Red, pero ninguna de las empresas de Internet se molestaba porque en realidad no les importaba y no tenían forma de facturar por su esfuerzo al usuario. Esto solo cambió cuando también lo hizo la economía de los correos electrónicos. Una vez que casi todo el mundo tuvo cuenta en uno de los pocos grandes proveedores de correo electrónico y la mayoría de los correos electrónicos pasaba por ellos, de pronto tenía sentido proporcionar servicios antispam a todos sus usuarios de manera automática. El resultado fue una serie de tecnologías que detectaron y pusieron en cuarentena al spam. Hoy en día, el spam sigue constituyendo algo

más de la mitad de todos los correos electrónicos,[1] pero el 99,99 % está bloqueado.[2] Es una de las historias de éxito de la seguridad informática.

Ahora piensa en el fraude con las tarjetas de crédito. En los inicios de las tarjetas, los costes del fraude los sufragaban los consumidores, lo que dio como resultado que los bancos hicieran poco para evitarlos. Esto cambió en 1974, cuando Estados Unidos promulgó la Ley de Facturación Justa de Crédito, que limitaba la responsabilidad del consumidor a los primeros cincuenta dólares. Al obligar a los bancos a pagar los costes del fraude, el Congreso ofreció un incentivo para acabar con él. El resultado fueron todas las medidas antifraude que todavía se aplican: verificación de tarjetas en tiempo real, sistemas integrales expertos que buscan señales de fraude, requisitos de activación manual de tarjetas, chips en las tarjetas, etc. Todas estas medidas redujeron el fraude general, y, lo que es más importante, no era algo que los clientes pudieran haber hecho por sí mismos. Los bancos del Reino Unido fueron capaces de repercutir los costes del fraude a los consumidores, por lo que fueron más lentos a la hora de adoptar estas medidas. Las directivas de servicios de pago de la Unión Europea han tratado de alinear más la protección del consumidor con los estándares estadounidenses, pero han dejado cierto margen de maniobra para que los bancos atribuyan a los clientes casos flagrantes de negligencia.[3] (Sorprendentemente, el Reino Unido puede hacer que esto empeore.)[4] De manera similar, en Estados Unidos las tarjetas de débito no se protegieron hasta que otra ley obligó a los bancos a pagar los costes del fraude, tal y como hicieron con las tarjetas de crédito.[5]

En ambos ejemplos, una vez obtenidos los incentivos para la seguridad, las tecnologías se implementaron para que esto sucediera. Con el spam hubo que modificar el ecosistema del correo electrónico para cambiar las motivaciones de los proveedores. Con las tarjetas de crédito fue necesaria una ley para cambiar los incentivos de los bancos. De igual forma, la seguridad de Internet+ es en esencia un problema de incentivos y de políticas.

Hasta ahora hemos dejado solos al mercado y al Gobierno, con capacidades de operar en secreto, quienes se han conformado con la situación de la que hablaba en la primera parte. Este es el estado insatisfactorio de la seguridad con las políticas actuales que tenemos implementadas. No mejorarán las cosas en el mercado mientras se obtengan más beneficios a corto plazo espiándonos y vendiendo nuestros datos, ocultándoles los detalles de seguridad a consumidores y usuarios e ignorando la seguridad y esperando que pase lo mejor. Los Gobiernos no mejorarán las cosas mientras estén

controlados en gran medida por grupos de presión corporativos y por organizaciones como la NSA y el Departamento de Justicia estadounidenses, que prefieren el espionaje a la seguridad.

Si queremos cambiar el balance de las pérdidas debidas a la falta de seguridad y los gastos por mejoras en esa seguridad, tendremos que cambiar los incentivos. Serán nuestros Gobiernos representativos, trabajando de manera transparente, los que cambiarán las cosas para mejor; ellos son hoy la pieza faltante en la seguridad de Internet+. Aunque seguro que habrá todo tipo de problemas para lograrlo, no veo ninguna otra forma de que funcione. La participación del Gobierno, ya sea en forma de regulación, compromiso o financiamiento directo, no es la panacea, pero tampoco lo es su ausencia. En el mejor de los casos, el Gobierno nos permite a todos superar problemas de acción colectiva, financiar esfuerzos que no enfatizan los resultados a corto plazo y establecer los fundamentos de lo que es un comportamiento aceptable. En el peor de los casos, el Gobierno se basa en intereses privados o se convierte en una burocracia enquistada más preocupada por su propia supervivencia que por gobernar. La realidad es probable que se encuentre en algún lugar en medio de esos dos escenarios.

En mi libro sobre la confianza *Liars and Outliers* (*Mentirosos y valores atípicos*) decía que «la seguridad es un impuesto para los honestos».[6] En general, me refiero a los costes adicionales en que incurrimos todos porque algunos no somos honestos. Estos costes se repercuten en un precio de los artículos más alto porque los propietarios de las tiendas han tenido que contratar guardias e instalar cámaras de seguridad para lidiar con los hurtos.

El gasto en seguridad es una especie de peso muerto: no supone nada productivo, pero reduce lo malo que podría suceder. Si los bancos no tuvieran que gastar dinero en seguridad, sus servicios podrían ser más baratos; si los Gobiernos no tuvieran que gastar dinero en la policía o el ejército, podrían reducir los impuestos, y si tú y yo no tuviéramos que preocuparnos por los ladrones, podríamos ahorrar dinero al no tener que comprar cerraduras de puertas, alarmas contra robos ni barrotes para las ventanas. En algunos países, algo así como una cuarta parte de todo el trabajo puede definirse como trabajo de vigilancia.[7]

La seguridad de Internet+ no es diferente. La firma de análisis de tecnología Gartner estima que el gasto en seguridad de Internet en todo el mundo durante 2018 fue de 100.000 millones de dólares.[8] Si queremos más seguridad, tendremos que gastar dinero para conseguirla: pagar precios más altos por nuestros ordenadores, teléfonos, dispositivos IoT, servicios de

Internet y todo lo demás; no hay otra opción. Las políticas establecerán cómo vamos a pagarlo.[9]

A veces tiene sentido que paguemos por la seguridad de forma individual. La seguridad del hogar funciona de esa manera. Cada uno compra su propia cerradura de puerta, y algunos también instalan sistemas de alarma antirrobo, otros gastan su dinero en armas para sus hogares y tal vez los más ricos paguen por guardaespaldas, habitaciones del pánico o, si se trata de un villano de James Bond, secuaces. Estos son todos los gastos posibles, pero son personales. Lo que sea que decidas hacer no me afecta, y lo que yo haga no te afecta a ti.

A veces tiene sentido que paguemos la seguridad colectivamente. La vigilancia funciona de esa manera. No decimos «Si quieres un poco de vigilancia entonces págala tú mismo». En vez de eso, una parte de los impuestos que todos pagamos se destina a los servicios de policía de la comunidad. Hacemos esto porque los beneficios comunes se prestan de manera más efectiva mediante la toma de decisiones y la financiación colectivas. La policía protege a la sociedad en general (al menos en teoría), con independencia de que individuos específicos quieran protección.

Al final, nuestra seguridad mejorada para Internet+ probablemente sea una mezcla de gastos individuales y colectivos, de los cuales hablaremos en esta segunda parte. Los gastos individuales incluirán programas de seguridad para nuestros ordenadores y cortafuegos para nuestras redes. Los gastos colectivos abarcarán investigaciones policiales de delitos informáticos, unidades militares de guerra cibernética e inversiones en infraestructura de Internet. Las empresas incorporarán seguridad a sus productos, ya sea porque el mercado lo exija o porque el Gobierno las obligue a hacerlo. Habrá demandas donde haya inseguridad, seguros para protegerse contra pérdidas y un aumento de seguridad resultante de prevenir las demandas y reducir las primas de los seguros. No será una única cosa, sino un mosaico de muchas, igual que la seguridad en el mundo real.

Va a ser caro, pero ese es el tema: ya lo estamos pagando de todos modos. Es difícil encontrar cifras válidas sobre cuánto cuesta la inseguridad de Internet, pero tenemos un rango. Un informe de 2017 del Instituto Ponemon concluyó que una de cada cuatro compañías será hackeada, con un coste promedio de 3,6 millones de dólares cada una.[10] Otro informe de Symantec estimó que 978 millones de personas en veinte países se vieron afectadas por la ciberdelincuencia en 2017, con un coste de 172.000 millones de dólares.[11]

Un estudio realizado por RAND en 2018 ofreció el análisis más completo que he visto y los resultados están por todo el mapa:

> Encontramos que los valores resultantes son altamente sensibles a los parámetros de entrada. Por ejemplo, al utilizar tres conjuntos razonables de parámetros de la investigación existente y nuestro propio análisis de datos, encontramos que el delito cibernético tiene un coste directo en el producto interno bruto (PIB) de 275.000 millones de dólares y de 6,6 billones a nivel mundial, y que los costes totales del PIB (directos más sistémicos) son de entre 799.000 millones y 22,5 billones de dólares (1,1 % a 32,4 % del PIB).[12]

Con independencia de la estimación que utilicemos, es mucho dinero. Y ese coste será un lastre para la economía, ya sea pagando pérdidas o medidas de seguridad diseñadas para minimizarlas. Todo lo que gastamos en pérdidas se desperdicia, pero todo lo que pagamos por una seguridad mejorada se traduce en mejores tecnologías de seguridad, menos delincuentes, prácticas corporativas más seguras, etc., y todo esto continuará dando sus frutos año tras año.

Hay una broma que dice que los tecnólogos recurren a la ley para resolver sus problemas, mientras que los abogados recurren a la tecnología para resolver los suyos. En realidad, para lograr que todo esto funcione, la tecnología y la ley tendrán que trabajar juntas. Esta es la lección más importante que nos dejan los documentos de Edward Snowden. Siempre supimos que la tecnología podía subvertir la ley. Snowden nos mostró que la ley, sobre todo la secreta, también puede subvertir la tecnología. Ambas deben trabajar juntas o ninguna funcionará.

Esta segunda parte describe cómo podemos conseguirlo.

06

CÓMO ES UN INTERNET+ SEGURO

EN 2016, EL CONSEJO DE CONSUMIDORES Noruego evaluó tres muñecas conectadas a Internet. El grupo descubrió que las condiciones de uso y las políticas de privacidad de las compañías mostraban una «desconcertante falta de respeto por los derechos básicos de los consumidores y de la privacidad», eran «generalmente vagos acerca de la retención de datos» y que dos de los juguetes «transfieren información personal a un tercero comercial que se reserva el derecho de utilizar esta información para prácticamente cualquier propósito, sin relación con la funcionalidad de los juguetes en sí mismos».[1] Pero se agrava:

> Se descubrió que dos de los juguetes no tenían prácticamente seguridad incorporada. Esto significa que cualquier persona podía obtener acceso al micrófono y los altavoces dentro de los juguetes, sin necesidad de acceso físico a los productos […].
>
> Además, las pruebas encontraron evidencias de que los datos de voz se estaban transfiriendo a una compañía en Estados Unidos que también se especializaba en la recopilación de datos biométricos como el reconocimiento de voz. Finalmente, se reveló que dos de los juguetes tenían incorporadas frases preprogramadas que respaldaban diferentes productos comerciales, lo que prácticamente constituía publicidad indirecta de productos dentro de los propios juguetes.

Utilizo como demostración una de las muñecas, Mi Amiga Cayla, en la clase de Políticas de Seguridad de Internet que imparto en Harvard Kennedy School. Es ridículamente fácil de hackear, incluso para mis estudiantes no técnicos. Todo lo que tienen que hacer es abrir el panel de control de bluetooth de sus teléfonos y conectarse a la muñeca desde sus asientos. Entonces pueden escuchar lo que oye el juguete y enviar mensajes a través de sus altavoces. Es una demostración superespeluznante de lo mala que puede ser la seguridad de un producto comercial. Alemania prohibió a Mi Amiga

Cayla porque, efectivamente, es un dispositivo de escucha que dejaba desprotegido en Internet el audio que había grabado,[2] si bien todavía está a la venta en otros países. Y no sucede solo con esta muñeca: Hello Barbie de Mattel tuvo problemas similares.[3]

En 2017, la agencia de informes crediticios al consumidor Equifax anunció que a 150 millones de estadounidenses, poco menos de la mitad de la población, les habían robado sus datos personales.[4] Los atacantes obtuvieron acceso a nombres completos, números de la seguridad social, fechas de nacimiento, direcciones y números de permisos de conducir, justo la información necesaria para cometer los fraudes de robo de identidad mencionados en el capítulo 4. No fue un ataque sofisticado, y aún no tenemos la menor idea de quién lo hizo. Los atacantes utilizaron una vulnerabilidad crítica en el software de la página web de Apache que habían reparado dos meses antes.[5] Equifax había sido informado por Apache, el CERT (Equipo de Respuesta ante Emergencias Informáticas) y el Departamento de Seguridad Nacional estadounidenses sobre la vulnerabilidad,[6] pero no logró instalar el parche hasta meses después de que los atacantes accedieran a la red.[7] El riesgo de la empresa era increíble.[8] Cuando declaré sobre este asunto ante el Comité de Energía y Comercio de la Cámara de Representantes, la llamé «ridículamente mala».[9] Y no fue un incidente aislado: Equifax tenía un historial de fallos de seguridad.[10]

Ojalá fueran historias excepcionales, pero no lo son. De verdad va todo muy mal ahí afuera, y sin una intervención seria, nada mejorará.

En pocas palabras, lo que tenemos que hacer es construir *seguridad de diseño*.[11] Por las razones de ingeniería discutidas en el capítulo 1 y las razones políticas o de mercado que se discutieron en el capítulo 4, con frecuencia la seguridad queda por detrás de la velocidad del desarrollo y de las demás funciones. Incluso para las empresas más grandes, que deberían saberlo mejor que nadie, la seguridad informática suele considerarse como un ejercicio de cumplimiento que frena el desarrollo y añade gastos. Es algo que se ha metido con calzador al final de un proceso de desarrollo, de forma apresurada y no muy eficaz. Esto es algo que tiene que cambiar. La seguridad debe diseñarse desde el principio para cada sistema y para cada componente, y durante todo el proceso de desarrollo.

Admito que esto suena obvio, pero hay que recordar que la seguridad no es algo que se diseñase en Internet desde el principio, y no es algo que el mercado generalmente recompense. Es un poco como el proceso lento mediante el cual todos convencimos a las empresas de automóviles, a través

de la regulación y la presión del mercado, a adoptar la eficiencia de combustible por diseño.

Las industrias muy reguladas, como las de aviónica y de dispositivos médicos, ya emplean la seguridad en su diseño. También está presente en las aplicaciones bancarias y en las de compañías de sistemas operativos, como Apple y Microsoft. Aunque la práctica necesita extenderse más allá de estos casos aislados.

Necesitamos proteger Internet+, nuestro software, datos y algoritmos, y la infraestructura crítica y la cadena de suministro informático; necesitamos hacerlo de manera integral y necesitamos hacerlo ahora. Este capítulo trata de elaborar algunas líneas generales de cómo podría hacerse esto. Me estoy centrando en el qué y dejando el cómo y el quién para los siguientes dos capítulos.

Para ser justos, estos son solo los elementos básicos y hay muchas sutilezas en las amenazas analizadas en la primera parte que no abordaré en absoluto. Las recomendaciones en este capítulo no pretenden ser definitivas; son un punto de partida para la discusión. Todos los principios propuestos aquí deben ampliarse y, finalmente, abrirse camino hacia estándares voluntarios u obligatorios de la industria.

Pero si no empezamos en alguna parte, nunca llegaremos a lo complicado.

PROTEGER NUESTROS DISPOSITIVOS

En los inicios de Internet, tenía sentido dejar que algo se conectara a él, pero eso ya no es sostenible. Necesitamos establecer estándares de seguridad para ordenadores, software y dispositivos. Tal vez suene fácil, pero no lo es. Debido a que el software está ahora integrado en cada cosa, esto rápidamente se convierte en estándares de seguridad que lo abarcan todo (lo cual es demasiado amplio para ser razonable).

Aunque, si todo es un ordenador, tenemos que pensar en principios de diseño holístico. Todos los dispositivos deben ser seguros sin demasiada intervención de los usuarios, y, aunque está bien tener diferentes niveles de seguridad como respuesta a amenazas distintas, estos deberían tener una base común.

Para ello, ofrezco diez principios de diseño de alto nivel para mejorar tanto la seguridad como la privacidad de nuestros dispositivos. Si bien estos no son lo suficientemente específicos para ser estándares, son una base a partir de la cual pueden desarrollarse.

1. Transparencia. Los proveedores deben indicar con claridad cómo funciona su seguridad, contra qué amenazas protegen y contra cuáles no, y así sucesivamente. Si un proveedor ya no admite un dispositivo después de cierta fecha, debe informar a los clientes con la suficiente antelación para permitir una planificación adecuada de la actualización.
2. Hacer que el software sea parcheable. Todos los dispositivos deben tener la capacidad de aceptar actualizaciones de software y firmware, además de una forma de autenticarlos como válidos. Los proveedores también deben instalar parches rápidamente una vez que se descubran las vulnerabilidades, y los productos deben poder verificar periódicamente si hay actualizaciones. Esto es vital: incluso a pesar de todos los problemas con los parches mencionados en el capítulo 2, el software no parcheable es aún peor.
3. Probar antes de producir. Se debe probar la seguridad de todo el software antes de su lanzamiento.
4. Habilitar la operación segura por defecto. Los dispositivos deben ser seguros sin necesidad de que los usuarios los configuren. No deben tener contraseñas débiles o predeterminadas, la autenticación de dos factores debe usarse siempre que sea posible y las funciones de administración remota deben desactivarse a menos que sea necesario.
5. Fallar predeciblemente y con seguridad. Si un dispositivo pierde la conexión a Internet, debería fallar de una manera que no cause ningún daño.
6. Utilizar protocolos e implementaciones estándares. Los protocolos estándar son por lo general más seguros y están mejor probados, y los protocolos personalizados todo lo contrario. Los dispositivos deben utilizar protocolos e implementaciones de comunicaciones estándar y deben ser interoperables con otras aplicaciones y dispositivos. Los proveedores no deben crear sus propios protocolos a menos que no haya otra opción.
7. Evitar las vulnerabilidades conocidas. Los proveedores no deben enviar productos que contengan vulnerabilidades conocidas.
8. Preservar la funcionalidad fuera de línea. Los usuarios deben poder desactivar todas las conexiones de red entrantes y salientes mientras puedan usar el dispositivo. Por ejemplo, un frigorífico conectado a

Internet debe mantener las cosas frías incluso cuando no esté conectado a Internet.

9. Cifrar y autenticar datos. Los datos deben estar cifrados en los dispositivos y las comunicaciones hacia y desde ellos deben estar cifradas y autenticadas.
10. Apoyar la investigación de seguridad responsable. Los proveedores deben permitir la investigación de sus productos y apreciar los informes de vulnerabilidad, no acosar a los investigadores.

Estos principios y algunos de los elementos de la siguiente sección proceden de un grupo de trabajo sobre seguridad nacional del cual soy miembro, organizado por el Centro Berkman Klein para Internet y la Sociedad y financiado por la Fundación Hewlett.[12]

Ninguno de estos principios es nuevo o innovador. Mientras investigaba para este libro reuní diecinueve pautas de seguridad y privacidad diferentes para el IoT, creadas por la IoT Security Foundation, la Online Trust Alliance, el estado de Nueva York y otras organizaciones;[13] todas son similares, lo que las convierte en una buena indicación de lo que los profesionales de la seguridad creen que debería hacerse, aunque todas son voluntarias, por lo que nadie las sigue en realidad.

PROTEGER NUESTROS DATOS

De igual forma que necesitamos principios de diseño de seguridad para ordenadores, también los necesitamos para datos. Antes ambos eran lo mismo, pero hoy están separados. Ya no almacenamos nuestros datos personales en ordenadores que están físicamente cerca, sino en la nube, en servidores masivos, propiedad de otros, que tal vez estén en otros países.

Con frecuencia nuestros datos también son propiedad de otros: los recopilan sin nuestro conocimiento o consentimiento. Estas bases de datos son objetivos tentadores para los atacantes de todas las clases. Necesitamos principios de seguridad que rodeen los datos y las bases de datos y que se aplicarían a todas las organizaciones con bases de datos personales:

1. Minimizar la recopilación de datos. Las empresas solo deben recopilar aquellos que necesiten y ningún otro.
2. Almacenar y transferir datos de forma segura. Estos datos deben estar protegidos, tanto en tránsito como en almacenamiento.

3. Minimizar el uso de datos. Solo deben usarse cuando sea esencial.
4. Ser transparente en la recopilación, uso, almacenamiento y eliminación de datos. Las empresas deben indicar claramente qué datos de los usuarios se recogen, cómo se almacenan y utilizan y cuándo se eliminan.
5. Hacer anónimos los datos siempre que sea posible. Si no es necesario identificar a los individuos, entonces sus datos deben ser anónimos.
6. Permitir a los usuarios acceder, inspeccionar, corregir y eliminar sus datos. Las empresas no deben mantener en secreto la información que tienen de las personas.
7. Eliminar los datos cuando ya no sean necesarios.

Será crucial para cualquier norma que proteja información personal saber en qué consiste esta. Tradicionalmente, es algo que hemos definido de manera limitada como información personal identificable, pero eso no es suficiente. Ahora sabemos que se puede combinar todo tipo de información para identificar a las personas y que hacer anonimizar los datos es mucho más difícil de lo que parece.[14] Necesitamos definiciones más amplias de lo que entendemos por información personal (por ejemplo, los datos de las aplicaciones en tu teléfono, e incluso la lista de complementos instalados en tu navegador) y, por lo tanto, ser conscientes de que es necesario protegerla.

Estos criterios aparecen en mi libro de 2015 *Data and Goliath* (*Datos y Goliat*). La mayoría de ellos forman parte del Reglamento General de Protección de Datos de la UE, del que hablaré en el capítulo 10. De nuevo, se trata de principios generales de diseño y probablemente sean los más difíciles de vender en este capítulo. Las empresas lucharán al verse obligadas a proteger sus dispositivos, pero a la larga esto las beneficiará. Las normas sobre la obtención de datos tienen el potencial de amenazar el capitalismo de vigilancia. Las empresas argumentarán que necesitan recopilar todos los datos para un posible análisis futuro, para capacitar a los sistemas de aprendizaje automático o porque podrían ser valiosos algún día, pero necesitaremos estas normas porque las bases de datos de información personal serán cada vez más grandes y más personales.

Gran parte de estos datos estarán en la nube. Esta tendencia es simple economía y constituirá el modelo informático en el futuro inmediato.[15] En muchos sentidos es algo bueno; de hecho, creo que las personas que mueven sus datos y los procesan en la nube son nuestra vía más fructífera para mejorar la seguridad. Hasta ahora, Google ya hace un trabajo mejor para

asegurar nuestros datos de lo que la mayoría de los individuos o pequeñas empresas podrían hacer por sí mismos. Los proveedores de servicios en la nube tienen tanto la experiencia en seguridad como las economías de escala de las que carecen los individuos y las pequeñas empresas, y cualquier cosa que ofrezca protección a las personas sin que tengan que convertirse en expertos en seguridad es una victoria.

Sin embargo, existen riesgos: tener múltiples usuarios diferentes en la misma red aumenta las oportunidades de piratería interna, y los grandes proveedores de la nube (como las grandes bases de datos de información personal) son objetivos atractivos para los atacantes poderosos. Necesitamos más investigación en seguridad en la nube. Si bien la mayoría de los principios mecionados con anterioridad están relacionados con los acumuladores de bases de datos personales, algunos también se aplican a proveedores de computación en la nube.

PROTEGER NUESTROS ALGORITMOS

Esperamos mucho de nuestros algoritmos y, dado que continúan reemplazando a los seres humanos en los procesos de toma de decisiones, vamos a tener que confiar totalmente en ellos. A un nivel alto, esperamos precisión, imparcialidad, reproducibilidad, respeto a los derechos humanos y otros derechos, y mucho más.[16] Me estoy centrando en la seguridad.

La amenaza es básicamente que un algoritmo se comporte de manera involuntaria, ya sea porque se haya programado mal o porque pirateen sus datos o software. La transparencia es una solución obvia: cuanto más transparente sea un algoritmo, más se puede inspeccionar y auditar, por seguridad o por cualquier otra propiedad que queramos que tengan nuestros algoritmos.

El problema es que la transparencia no siempre se consigue en los algoritmos, ni es deseable. Las empresas tienen secretos comerciales razonables que necesitan para mantener su confidencialidad, y la transparencia puede representar un riesgo para la seguridad, ya que les proporciona información a los atacantes que puede ayudarlos a controlar el sistema. Por ejemplo, conocer el algoritmo de Google para la clasificación de páginas puede ayudar a la gente a optimizar sus webs, pero conocer el algoritmo de los militares para identificar personas mediante drones puede ayudarlas a esconderse.

Además, la transparencia no siempre es suficiente. Los algoritmos modernos son tan complejos que ni siquiera es factible determinar si son exactos, por no decir justos o seguros. Algunos algoritmos de aprendizaje automático tienen modelos que están más allá de la comprensión humana.[17]

Este último punto es importante. A veces la transparencia es imposible. Nadie sabe cómo funcionan algunos algoritmos de aprendizaje automático, incluidos sus diseñadores; son fundamentalmente incomprensibles para los humanos. Piensa en ellos como si fueran cajas negras: los datos entran, las decisiones salen y lo que sucede en medio sigue siendo un misterio.[18]

Incluso aunque un algoritmo no pueda hacerse público, o si no hay manera de entender cómo funciona, podemos pedir que se explique;[19] es decir, podemos exigir que los algoritmos justifiquen sus razonamientos.[20] Así, por ejemplo, cuando un algoritmo realiza un diagnóstico médico o califica la idoneidad de un candidato para una tarea en particular, también se le puede pedir que justifique los motivos de sus decisiones.

Esto no es la panacea. Debido a la forma en la que funciona el aprendizaje automático, las explicaciones pueden no ser posibles o comprensibles para los humanos[21] y requerirlas a menudo reduce la precisión de los algoritmos subyacentes porque los obliga a ser más simples de lo que serían de otra manera.[22]

Es probable que lo que en realidad queramos sea responsabilidad[23] o que las explicaciones sean discutibles;[24] tal vez necesitemos la capacidad de inspeccionar un algoritmo o de interrogarlo con datos de muestra y examinar los resultados. Quizá todo lo que necesitemos sea la posibilidad de auditarlos.[25]

De otro modo, podemos tratar a los algoritmos como seres humanos. Los humanos son terribles para explicar su razonamiento, y nuestras decisiones están llenas de sesgos inconscientes. Con demasiada frecuencia, una explicación (una serie lógica de pasos tomados para llegar a una decisión) en realidad no es más que una justificación. Nuestro cerebro subconsciente toma la decisión, y el cerebro consciente la justifica con una explicación. La literatura psicológica está llena de estudios que lo demuestran.

Aun así, podemos evaluar los prejuicios de los humanos al observar su toma de decisiones. De manera parecida, podemos juzgar los algoritmos observando sus resultados. Después de todo, lo que queremos saber es si un algoritmo utilizado para calificar a los candidatos es sexista o si uno para tomar decisiones de libertad condicional es racista.[26] Y podríamos decidir que, para algunas aplicaciones, los algoritmos de aprendizaje automático no

son apropiados porque queremos más control sobre cómo se toma una decisión.

No tengo recomendaciones concretas sobre cómo podemos confiar en nuestros algoritmos porque esto es demasiado nuevo. Apenas estamos empezando a descubrir qué es posible y qué es plausible. En este momento nuestros objetivos deben ser una mayor transparencia y la posibilidad de explicar y auditar algoritmos.

PROTEGER NUESTRAS CONEXIONES DE RED

La mayoría de nosotros nos conectamos a la Red a través de uno o más proveedores de acceso a Internet (ISP, por sus siglas en inglés), grandes compañías y muy poderosas, como AT&T, Comcast, BT y China Telecom. Un informe de 2011 calculó que las veinticinco empresas de telecomunicaciones más importantes del mundo conectan el 80 % de todo el tráfico de Internet.[27] Esta centralización puede ser mala para las elecciones del consumidor, pero nos proporciona un beneficio potencial de seguridad. Debido a que los proveedores de acceso a Internet se ubican entre nuestros hogares y el resto de la Red, se encuentran en una posición única para ofrecer seguridad, sobre todo para los usuarios domésticos. Necesitamos, por tanto, algunos principios de seguridad para los proveedores de servicio de Internet:

1. Proporcionar una conexión segura a los consumidores. Los ISP deben hacer algo más que conectar a los consumidores a Internet, también necesitan proteger esa conexión. Hasta cierto punto pueden proporcionar un servidor de seguridad entre el usuario y el resto de Internet. Y en la medida en que las conexiones de los usuarios no estén encriptadas, pueden buscar malware. (Algunos proveedores ya están bloqueando la pornografía infantil de esta manera.)[28]

2. Ayudar a configurar los dispositivos de Internet de los usuarios. Sin duda, los ISP están en la mejor posición para garantizar que los rúters de los consumidores estén configurados de manera segura, pero también pueden ayudar a administrar la seguridad de todos los dispositivos de Internet conectados a ese rúter.[29]

3. Educar a los consumidores sobre las amenazas. Debido a que los ISP son las compañías que conectan a los consumidores a Internet, están en la mejor posición para educar a los consumidores sobre las amenazas de Internet.

4. Informar a los consumidores de las infecciones en su infraestructura. Como los ISP conectan a los consumidores a Internet, pueden controlar esa conexión para detectar signos de malware y otras infecciones. Deberían informar al consumidor cada vez que descubran una amenaza. En el futuro, es posible que los proveedores de servicios de Internet tengan la responsabilidad de impedir que los dispositivos inseguros de los consumidores se conecten a la Red.

5. Comunicar públicamente las estadísticas de incidentes de seguridad. Los proveedores de acceso a Internet ya saben cosas como la cantidad de spam, cuántos ordenadores están en peligro o los detalles de los ataques de denegación de servicio, etc. Deben publicar esa información en conjunto para preservar el anonimato de sus clientes individuales.

6. Trabajar con otros proveedores para compartir información sobre amenazas inminentes y en caso de emergencia. De nuevo, los ISP pueden aprender sobre los ataques y ayudarse mutuamente para mitigar sus efectos.

Esta lista se basa en un artículo de la consultora de seguridad cibernética Melissa Hathaway, asesora principal de políticas de los expresidentes George W. Bush y Barack Obama.[30]

Los principios propuestos otorgarían a los proveedores de acceso a Internet un poder considerable, lo que conlleva un peligro enorme. Si los ISP pueden configurar la seguridad de los usuarios, también pueden hacerlo para permitir el acceso del Gobierno. Y, si pueden discriminar entre diferentes tipos de tráfico, pueden violar la neutralidad de la Red por todo tipo de razones económicas o ideológicas. Estas son preocupaciones reales, y necesitamos mejores políticas para aliviarlas. Pero los usuarios no deberían tener que ser expertos en seguridad para usar Internet de manera segura, y los proveedores de acceso a Internet deberán actuar como una primera línea de defensa.

PROTEGER INTERNET

Heartbleed es el nombre que los investigadores le dieron a una grave vulnerabilidad en OpenSSL, el sistema de cifrado que protege tu navegación web. Si la conexión entre tu navegador y la web que estás leyendo está encriptada, es probable que sea obra de OpenSSL. El protocolo es público y el código es de fuente abierta. Heartbleed fue descubierto en 2014, dos años después de que se introdujera por accidente en el software. Supuso una gran vulnerabilidad (en su momento la llamé *catastrófica*)[31] que afectó

aproximadamente al 17 % de los servidores web de Internet[32] y los dispositivos de usuario final, desde servidores hasta cortafuegos y tomas de corriente.

La vulnerabilidad permitió a los atacantes encontrar nombres de usuario y contraseñas, números de cuenta y más. Arreglar Heartbleed fue una tarea gigantesca que requirió la coordinación entre sitios web, autoridades de certificación y compañías de navegadores web en todo el mundo. Hubo dos factores que precipitaron Heartbleed: uno, el hecho de que OpenSSL, una pieza crítica de software, la mantuviera una única persona y algunos ayudantes que trabajaban gratis en su tiempo libre, y dos, nadie había sometido a OpenSSL a un buen análisis de seguridad. Fue un problema de acción colectiva clásico. El código es de fuente abierta, por lo que cualquiera puede evaluarlo, pero todos pensaron que lo haría otro, por lo que nadie se esforzó en hacerlo en realidad. El resultado fue que la vulnerabilidad pasó desapercibida durante más de dos años.[33]

Como respuesta a Heartbleed, la industria creó algo llamado Iniciativa de Infraestructura Central.[34] Básicamente, las grandes empresas de tecnología se reunieron y establecieron un programa de prueba para software de código abierto en el que todos confiamos. Es una buena idea que debería haberse llevado a la práctica una década antes, pero no es suficiente.

En el capítulo 1 explicaba que Internet nunca se diseñó teniendo en cuenta la seguridad, lo que estaba bien cuando estaba sobre todo en instituciones de investigación y se usaba principalmente para la comunicación académica,[35] pero ya no está tan bien hoy, cuando Internet es compatible con gran parte de la infraestructura crítica del mundo.

Los proveedores de servicio de Internet hacen más que conectar a los consumidores a la red. Los ISP de nivel 1 administran la conexión troncal de Internet y operan las grandes redes de alta capacidad en todo el mundo. Son empresas de las que probablemente nunca hayas oído hablar, como Level 3, Cogent o GTT Communications, porque los usuarios finales no son sus clientes.[36] Estas compañías también pueden hacer más para proteger Internet:

1. Proporcionar información de enrutamiento auténtica y autorizada. ¿Recuerdas en el capítulo 1 cuando hablaba sobre el protocolo de puerta de enlace (BGP) y cómo los países pueden enrutar maliciosamente el tráfico de Internet para contribuir al espionaje? Los proveedores de servicios de Internet son los que previenen esto.

2. Proporcionar información de nombres auténtica y autorizada para reducir el secuestro de nombres de dominio. Del mismo modo, los proveedores de servicios de Internet son los que pueden prevenir ataques maliciosos contra el sistema de nombres de dominio.

3. Comprometerse a tratar todo el tráfico por igual y no diferenciar el servicio basándose en el contenido de los datos.

Hay otras cosas que pueden hacer los ISP de nivel 1 que incluyen la supervisión del tráfico y la interceptación de ataques. Por ejemplo, podrían bloquear todo tipo de cosas: spam, pornografía infantil, ataques a Internet, etc. Sin embargo, todas estas cosas requieren en la actualidad que los proveedores de servicios de Internet se involucren en la vigilancia masiva del tráfico en la Red, y no funcionarán si el tráfico está encriptado. Y, dada la posibilidad, estamos mucho más seguros si el tráfico de Internet está cifrado de extremo a extremo. Hablaremos más sobre esto en el capítulo 9.

PROTEGER NUESTRA INFRAESTRUCTURA CRÍTICA

En 2008, hackers no identificados irrumpieron en el oleoducto Bakú-Tiflis-Ceyhan (Turquía). Obtuvieron acceso al sistema de control del conducto y aumentaron la presión del petróleo crudo que fluía hacia el interior, lo que provocó la explosión de la tubería.[37] También piratearon los sensores y las transmisiones de vídeo que controlaban la tubería para evitar que los operadores se enteraran de la explosión hasta cuarenta minutos después de que ocurriera. (¿Recuerdas lo que decía en el capítulo 1 sobre las nuevas vulnerabilidades en las interconexiones? Los atacantes entraron en los sistemas de control de los conductos a través de una vulnerabilidad en el software de comunicaciones de esas cámaras de vídeo).

En 2013, supimos que la NSA había pirateado la red de la compañía petrolera nacional de Brasil,[38] aunque el propósito era probablemente recabar información, y no atacar. Ya mencioné el ataque cibernético de Irán en 2012 contra Saudi Aramco, la compañía petrolera nacional de Arabia Saudí, y los ataques cibernéticos de 2015 y 2016 de Rusia contra la red eléctrica ucraniana. En 2017, alguien fue capaz de falsificar el GPS que los barcos utilizan para navegar y engañarlos sobre su ubicación.[39]

En el capítulo 4 decía que estamos en medio de una guerra cibernética cada vez más asimétrica. Con actores no estatales, como los terroristas, la asimetría es aún mayor; por lo que necesitamos proteger mejor nuestra infraestructura crítica en el ciberespacio.

Sin embargo, antes de que podamos hacerlo, tendremos que decidir qué definimos como *infraestructura crítica*. El término es complejo y ambiguo, y lo que cuenta está sujeto a cambios en los desarrollos tecnológicos y sociales. En Estados Unidos una serie de documentos de la Casa Blanca y del Departamento de Seguridad Nacional describen lo que el Gobierno considera infraestructura crítica.[40] Una directiva presidencial de 2013 identificó dieciséis sectores de infraestructura crítica.[41] Gran parte de lo que se incluye es obvio, como el transporte aéreo, la producción y el almacenamiento de petróleo y la distribución de alimentos. Otros tienen menos sentido, como centros comerciales y grandes estadios deportivos. Sí, son sitios donde se reúne una gran cantidad de personas y sería una tragedia nacional si una bomba matara a cientos o miles de personas en cualquiera de esos lugares, pero no parecen críticos de la misma manera en que lo es la red eléctrica.

Si todo es una prioridad, entonces nada lo es. Tenemos que tomar algunas decisiones difíciles y designar ciertos sectores como más vitales que otros. La Estrategia de Seguridad Nacional de Estados Unidos de 2017 identificó seis áreas clave: seguridad nacional, comunicaciones, transporte, luz y energía, banca y finanzas, salud y seguridad.[42] Algunas personas incluyen los sistemas electorales.[43] Creo que la energía, las finanzas y las telecomunicaciones son los primeros en los que hay que centrarse, porque sustentan todo lo demás. Si estamos buscando dónde encontrar la mayoría de los riesgos catastróficos a corto plazo analizados en el capítulo 5, ahí están. Y es donde obtendremos la mayor seguridad para nuestro dinero.

¿Por qué no estamos haciendo más por asegurar una infraestructura crítica hoy? Existen varias razones:

Una, es caro. El modelo de amenazas contra el que tenemos que defendernos suele ser una sofisticada unidad militar extranjera que ataca a profesionales altamente cualificados. Esto no es sencillo ni barato.

Dos, es fácil para la gente y los responsables de las políticas descartar futuros riesgos hipotéticos. Hasta que los ciudadanos de Estados Unidos experimenten un ataque cibernético real contra la infraestructura crítica en su país, ni el ataque de Corea del Norte contra Sony ni los ataques contra otros países como Arabia Saudí y Estonia cuentan aquí ni serán una prioridad.

Tres, el proceso político es complicado. El presidente Obama designó dieciséis amplios sectores como parte de nuestra infraestructura crítica para garantizar que todas las industrias se sintieran debidamente reconocidas. Cualquier intento por priorizar se encontrará con la resistencia de industrias que se sienten menospreciadas por una clasificación más baja. Entonces,

aunque a mí me resulte fácil decir que nuestra red eléctrica y nuestra infraestructura de telecomunicaciones deben protegerse primero porque todo lo demás está construido sobre ellas, es más difícil para el Gobierno decir lo mismo.

Cuatro, el Gobierno no tiene control directo sobre la mayor parte de nuestra infraestructura crítica. A menudo escucharás que el 85 % de la infraestructura crítica de Estados Unidos está en manos corporativas. Esa estadística proviene de un documento de 2002 de la Oficina de Seguridad Nacional[44] y parece ser una estimación aproximada.[45] Desde luego, depende de la industria de la que estemos hablando.[46] Como he explicado antes, es más probable que los propietarios privados subestimen la seguridad porque es más rentable ahorrar dinero cada año y arriesgarse.

Y cinco, gastar dinero en infraestructuras no es atractivo. Incluso cuando un país promociona sus inversiones en infraestructura, por lo general esto significa construir puentes nuevos y brillantes en lugar de reparar los viejos y destartalados. A pesar de que los presidentes Obama y Trump promocionen sus inversiones en infraestructura, el gasto para mantener lo que ya existe no es una prioridad, solo tienes que fijarte en nuestra infraestructura nacional en muchas áreas. Y puede ser aún peor cuando se trata de seguridad. Estos gastos son a largo plazo y es difícil atribuirse el mérito. Para cuando se evidencia que el gasto estaba justificado, el político que lo aprobó podría no estar ya en su cargo.

El hecho de que necesitemos proteger nuestra infraestructura crítica del ataque cibernético no es una idea nueva ni controvertida, y los Gobiernos, los grupos de la industria y el mundo académico han realizado muchos estudios sobre el tema;[47] sin embargo, los desafíos son considerables. No estoy discutiendo detalles porque este libro está destinado a ser general, pero cualquier defensa tendrá que ser necesariamente dinámica y debe integrar una gran variedad de personas, organizaciones, datos y capacidades técnicas. Nuestra infraestructura está formada por sistemas complejos con miles de millones de subsistemas y subcomponentes, algunos de los cuales han existido durante décadas. Arreglar cualquiera de estos será costoso, pero es factible.

DESCONECTAR SISTEMAS

Uno de los documentos clasificados de la NSA revelado por Edward Snowden era una presentación que contenía una diapositiva con el lema del

entonces director de la NSA Keith Alexander: «Guárdalo todo».[48] Un lema similar para Internet+ hoy podría ser: «Conéctalo todo», aunque tal vez no sea una buena idea.

Necesitamos empezar a desconectar equipos. Si no podemos proteger sistemas complejos en el grado en que lo requieran sus capacidades en el mundo real, no debemos construir un mundo donde todo esté informatizado e interconectado. Es parte de lo que quería decir cuando hablaba sobre ingeniería de seguridad por diseño al principio de este capítulo: si estamos construyendo un equipo y la única forma de protegerlo es no conectándolo, debe tenerse en cuenta como una opción válida.

Esto podría considerarse como una herejía en la actual carrera por conectarlo todo, pero los grandes sistemas centralizados no son inevitables. Las elites técnicas y corporativas pueden estar empujándonos en esa dirección, pero en realidad no tienen ningún otro argumento de apoyo que no sea la maximización de las ganancias.

Esta desconexión puede darse de varias formas: puede conllevar la creación de redes seguras físicamente aisladas de aquellas que han demostrado no ser seguras (aunque estas también tienen vulnerabilidades y no son la panacea de la seguridad), puede significar volver a sistemas no interoperables y, para empezar, puede suponer no crear conectividad para los sistemas. También hay formas graduales de hacer esto, como habilitando solo las comunicaciones locales, diseñando dispositivos específicos, invirtiendo la tendencia actual de convertirlo todo en un ordenador de propósito general, avanzando hacia una menor centralización y sistemas más distribuidos, que es como se imaginó Internet en primer lugar.

Vale la pena explicar esto. Antes de Internet, la red telefónica era inteligente. Los complejos algoritmos de enrutamiento de llamadas se encontraban dentro de la red, mientras que los teléfonos que se conectaban a ella eran estúpidos. Antes de Internet este también era el modelo de otras redes informatizadas, pero Internet le dio la vuelta. La mayor parte de la inteligencia se trasladó a los ordenadores que intervienen en la comunicación, y la red se hizo lo más tonta posible, un cambio que convirtió a Internet en un foco de innovación. Cualquiera podía inventarse algo nuevo: un software, un modo de comunicación o un dispositivo de hardware, y podía conectarse siempre y cuando se ajustara a los protocolos básicos de Internet. No hubo procesos de certificación, ni sistemas de aprobación centralizados: nada. Dispositivos inteligentes; red tonta. Para los estudiantes de la arquitectura de Internet, esto se conoce como *principio de extremo a extremo*.[49] Y, por

cierto, es lo que todos los que están a favor de la neutralidad de la Red quieren conservar.[50]

Anticipo que, con el tiempo, alcanzaremos un elevado grado de informatización y de conectividad, y luego habrá una reacción. No será impulsada por el mercado, sino por normas y leyes y por decisiones políticas que sitúen la seguridad y el bienestar de la sociedad por encima de corporaciones e industrias individuales. Requerirá un cambio social importante, y uno difícil de tragar para muchos, pero nuestra seguridad dependerá de ello.

De ahí en adelante tomaremos decisiones conscientes sobre qué y cómo nos interconectamos. Podemos establecer una analogía con la energía nuclear. A principios de la década de los ochenta, hubo un aumento dramático en el uso de la energía nuclear, antes de que reconociéramos que era demasiado difícil y peligroso protegernos de los desechos nucleares. Hoy en día, todavía tenemos energía nuclear, pero hay una mayor reflexión sobre cuándo y dónde construir plantas nucleares y cuándo elegir una de las muchas alternativas. Algún día la informatización será así.

Pero no hoy. Todavía estamos en la fase de luna de miel de la conectividad. Los Gobiernos y las corporaciones están totalmente ebrios de nuestros datos, y la prisa por conectarlo todo se debe a un deseo aún mayor de poder y participación de mercado.

07

CÓMO PODEMOS PROTEGER INTERNET+

POR LO GENERAL, las tecnologías ya existen para satisfacer todos los principios del capítulo anterior. Sí, quedan vulnerabilidades. Sí, hay problemas de usabilidad con algunas de esas soluciones. Pero en su mayor parte estos son principios de seguridad de sentido común que podrían implementarse hoy si hubiera algún aliciente para que las empresas lo hicieran.

Necesitamos crear ese incentivo elaborando políticas públicas sólidas. Hay básicamente cuatro puntos donde la política puede ejercer su influencia en la sociedad. El primero es *ex ante*: las reglas que intentan evitar que sucedan cosas malas; incluyen regulaciones sobre productos y categorías de productos, licencias de profesionales y productos, requisitos de prueba y certificación, y las mejores prácticas de la industria, además de subsidios o beneficios fiscales por hacer las cosas bien. El segundo es *ex post*: las reglas que castigan el mal comportamiento después de que ya haya ocurrido; comprenden multas por inseguridades y atribución de responsabilidades cuando las cosas salen mal. El tercero es exigir la divulgación: leyes de etiquetado de productos y otras medidas de transparencia, agencias de evaluación y calificación, intercambio de información entre el Gobierno y la industria, y leyes de divulgación de incumplimiento (algunas de estas revelaciones son *ex ante* y otras son *ex post*). Y la cuarta es la que clasificaría en términos generales como medidas que afectan al medioambiente; engloban el diseño deliberado del mercado, la financiación para investigación y educación, y el uso del proceso de adquisición como un medio para impulsar la mejora del producto de manera más amplia. Esta es la caja de herramientas, lo que tenemos para trabajar.

El objetivo de este tipo de políticas no es exigir que todo se proteja, sino crear incentivos para que exista un comportamiento seguro. Se trata de aumentar los costes de la inseguridad o (con menos frecuencia) reducir el coste de la seguridad.

Algo crítico para cualquier política es el proceso de ejecución. Las normas pueden ser aplicadas por el Gobierno, por organizaciones profesionales, por grupos de la industria o por terceros mediante la coacción o la presión del mercado. Hay cuatro formas básicas de aplicar las políticas de seguridad de Internet+.[1] Una, a través de normas como las de mejores prácticas; las normas proporcionan un punto de referencia que los grupos de defensa del consumidor, los medios de comunicación y los accionistas corporativos pueden utilizar para exigir que las empresas las tengan en cuenta. Dos, de forma voluntaria, a través de la autorregulación; a veces los organismos profesionales e industriales tienen interés en crear y hacer cumplir normas voluntarias, ya que sirven para aumentar la confianza de los consumidores y constituyen una barrera protectora de entrada para nuevos competidores. Tres, a través del litigio; si los clientes o las empresas pueden demandar cuando sufren daños, las empresas aumentan su seguridad para evitar esos juicios. Cuatro, a través de organismos reguladores; los organismos gubernamentales con el poder de emitir multas, de reclamar demandas o de obligar a las empresas a reparar los defectos pueden hacer cumplir estas normas.

Las cuestiones políticas pueden empujarnos hacia un conjunto particular de principios de gestión por defecto. Por ejemplo, espero demostrar que el Gobierno debe desempeñar un papel importante en todas estas iniciativas políticas, aunque otros prefieren iniciativas más dirigidas por el mercado. Otras opciones incluyen pautas gubernamentales no vinculantes, estándares de mejores prácticas voluntarias y acuerdos internacionales de múltiples partes interesadas, pero de esto hablaremos en el capítulo 8. En este me centraré en el cómo, sin preocuparme por quién lo hará.

Ninguna de las medidas que propongo en este capítulo son suficientes por sí solas. Los estándares mínimos de seguridad no lo resolverán todo, ni tampoco las responsabilidades. Eso está bien, sin embargo, porque ninguno de ellos trabajará de forma aislada, sino que todas las sugerencias de este capítulo interactuarán entre ellas, a veces de manera complementaria y otras de manera contradictoria. Si vamos a proteger Internet+, será a través de una serie de políticas que se refuercen mutuamente, como todo lo demás en la sociedad.

CREAR ESTÁNDARES

En primer lugar, debemos crear estándares reales para muchos de los principios enumerados en el capítulo 6.

Utilizo a propósito el término *estándar* y referido a las políticas. Existe una distinción en la ley acerca de las reglas prescriptivas, que son rígidas, y los estándares, basados en principios más flexibles.[2] Los estándares permiten la elección o la discreción, pueden proporcionar un marco para equilibrar varios factores diferentes y adaptarse a las circunstancias cambiantes. Entonces, mientras que una regla puede ser que el límite de velocidad en la nieve sea de 56 k/h, un estándar puede ser tener cuidado cuando está nevando. En la seguridad de Internet+, las reglas rígidas podrían incluir que los consumidores tengan la capacidad de revisar sus datos personales y habilitar las operaciones predeterminadas seguras. Un estándar que requiere que el propietario de una base de datos tenga el debido cuidado para proteger su información personal deja mucho espacio para la interpretación, y el significado puede cambiar a medida que cambia la tecnología.

Otro estándar de Internet+ podría incluir el principio de que los proveedores de IoT deben esforzarse al máximo para no vender productos desprotegidos, lo que puede sonar vago, pero es un estándar legal real en el caso de que se piratee un dispositivo de IoT y los reguladores puedan demostrar que los fabricantes utilizan protocolos inseguros, no cifran sus datos y habilitan contraseñas predeterminadas. Entonces, obviamente, no han hecho todo lo que podían. Si hicieron todas esas cosas y más, y un pirata informático encontró una vulnerabilidad que no podía predecirse o prevenir de manera razonable, es posible que no se consideren culpables.

Tal vez necesitemos reglas y normas; no obstante, su aplicación estará sujeta a una normativa más flexible. Mi suposición es que, en el mundo dinámico de la seguridad de Internet+, la mayoría de las regulaciones se darán en forma de normas basadas en principios, y no en reglas rígidas.

Habrá necesariamente diferentes estándares para diferentes tipos de cosas. Por ejemplo, no trataremos cosas grandes y caras, como un frigorífico, de la misma manera que trataremos cosas desechables de bajo coste, como una bombilla. Si este último objeto tiene una vulnerabilidad, lo correcto es deshacerse de él y comprar uno nuevo, lo que tal vez obligue al fabricante a asumir los costes del cambio. Los frigoríficos son diferentes, pero también es probable que haya menos productores, por lo que será más fácil imponerles normas.

En general, es mucho más efectivo centrarse en los resultados que en los procedimientos. Se conoce como *regulación basada en resultados* y es cada vez más común en la mayoría de las áreas, desde códigos de construcción hasta seguridad alimentaria y reducción de emisiones.[3] Por ejemplo, una

norma no debe prescribir la metodología de parches que debe tener un producto; eso es demasiado detallado y algo que el Gobierno no hace bien, en especial en un entorno tecnológico en rápida evolución. Es mejor pedir un resultado específico (que los productos de IoT deben tener una forma segura de parchear) y dejar que la industria descubra cómo conseguirlo. Este enfoque de la regulación estimula la innovación en lugar de inhibirla. Piensa en la diferencia entre exigir que los aparatos sean un tanto por ciento más eficientes el próximo año y especificar un diseño de ingeniería particular.[4]

También debemos estandarizar los protocolos de seguridad que deben seguir las empresas que utilizan dispositivos de Internet+. El Marco para la Mejora de la Ciberseguridad de la Infraestructura Crítica del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es un gran ejemplo de este tipo de norma:[5] una guía completa para que las organizaciones del sector privado evalúen de forma proactiva y minimicen sus riesgos en ciberseguridad.

Hay otros estándares importantes: aquellos que regulan los procesos de negocios, como la forma de prevenir, detectar y responder a los ataques cibernéticos. Si están bien realizados pueden incentivar a las empresas a mejorar su seguridad general de Internet y tomar mejores decisiones sobre qué tecnologías comprar y cómo usarlas. Aunque menos evidente, la estandarización de este tipo de procesos de negocios también facilita que los directivos compartan ideas, impongan requisitos a socios externos y vinculen los estándares de seguridad con los seguros, además de servir como modelo para mejores prácticas en los litigios, y los tribunales pueden referirse a ellas al tomar decisiones.

Por desgracia, el Marco de Ciberseguridad del NIST es solo voluntario en esta etapa, aunque está ganando terreno.[6] En 2017, se convirtió en obligatorio para los organismos federales estadounidenses. Hacerlo obligatorio para todos sería una victoria reglamentaria fácil.

En la misma línea, el Gobierno de Estados Unidos tiene algo que se llama FedRAMP, un proceso de autorización y evaluación de seguridad para servicios en la nube. También utiliza un estándar NIST, y se supone que los organismos federales compran a proveedores certificados.[7] Por supuesto, cualquier norma evolucionará con el tiempo, a medida que cambien las amenazas, aprendamos más sobre lo que es efectivo y lo que no lo es, las tecnologías se transformen y los dispositivos conectados a Internet se vuelvan más poderosos y dominantes.

CORREGIR LOS INCENTIVOS DESALINEADOS

Imagina un CEO al que se le presentan las siguientes opciones: puede gastar un 5 % adicional en el presupuesto de ciberseguridad para hacer que su red corporativa, productos o bases de datos de clientes sean más seguros, o puede ahorrar ese dinero y arriesgarse a que nada salga mal. Un CEO racional elegirá ahorrar dinero o gastarlo en nuevas funciones para competir en el mercado, y, si tiene mala suerte y sucede lo peor (piensa en Yahoo en 2016 o en Equifax en 2017), la mayoría de los costes de la inseguridad correrán a cargo de otras empresas. El CEO de Equifax no recibió su indemnización por despido de 5,2 millones de dólares porque renunció, pero mantuvo su pensión de 18,4 millones de dólares y es probable que también sus acciones.[8] Su apuesta fallida le costó a la compañía entre 130 millones y 210 millones de dólares, aunque eso no era relevante para él en aquel momento;[9] tampoco lo fue el hecho de que tomara una decisión equivocada a largo plazo para la empresa.

Este es el clásico dilema del prisionero. Si todas las compañías gastaran el dinero extra en seguridad, Wall Street aceptaría el gasto como normal, pero, si cada uno elige su propio interés a corto plazo, cualquier compañía que piense a largo plazo y gaste más será penalizada de inmediato, ya sea por los accionistas cuando sus beneficios sean más bajos o por los clientes cuando sus precios suban. Necesitamos coordinar de alguna forma a las empresas y convencerlas para que mejoren juntas la seguridad.

Las consideraciones económicas van más allá. Incluso aunque un CEO decida priorizar la seguridad sobre el beneficio a corto plazo, solo gastará el dinero suficiente para proteger el sistema hasta equiparar el valor de la empresa. Esto es importante. Sus modelos de recuperación ante desastres se construirán en torno a las pérdidas para la empresa, y no las pérdidas para el país o para los ciudadanos individuales. Y mientras que la pérdida máxima para la empresa sea todo lo que esta vale, los costes reales de un desastre pueden ser mucho mayores. El desastre de Deepwater Horizon le costó a la BP unos 60.000 millones de dólares,[10] pero los costes ambientales, de salud y económicos fueron mucho mayores. Si esa compañía hubiera sido más pequeña, habría salido del negocio mucho antes de que pagara todo ese dinero. Los gastos adicionales que una empresa evita pagar son las externalidades, y las asume la sociedad.

En esto también hay algo de psicología. Estamos predispuestos a preferir ganancias seguras más pequeñas en lugar de ganancias mayores que supongan

un riesgo, y posibles pérdidas más grandes antes que pérdidas menores seguras.[11] El gasto en seguridad preventiva es una pérdida segura baja: el coste de una mayor seguridad. Reducir el gasto es una pequeña ganancia segura. Tener una red, un servicio o un producto inseguro conlleva una gran pérdida. Esto no significa que nadie gaste dinero en seguridad, sino que es una batalla cuesta arriba superar este sesgo cognitivo, que explica por qué a menudo los CEO están dispuestos a arriesgarse.[12] Por supuesto, suponiendo que los primeros ejecutivos de las empresas estén bien informados sobre las amenazas, aunque la mayoría de ellos no lo están.

Esta disposición a asumir los riesgos de tener una red desprotegida se debe en parte a la falta de responsabilidades legales claras por producir productos inseguros, de los cuales hablaremos más extensamente en la próxima sección. Hace años bromeé diciendo que, si un producto de software mutilaba a uno de tus hijos, y el fabricante sabía que eso iba a ocurrir, pero decidió no decírtelo porque podría perjudicar sus ventas, no se vería como responsable. Ese chiste solo funcionó porque en aquel entonces el software no podía mutilar a uno de tus hijos.

Hay otras razones por las que los incentivos de seguridad no están alineados de forma adecuada. Las grandes empresas con pocos competidores no tienen muchos estímulos para mejorar la seguridad de sus productos porque los usuarios no tienen otra alternativa; o bien los compran (con problemas de seguridad y todo), o bien se quedan sin nada. Las pequeñas empresas tampoco tienen muchos alicientes, ya que ralentizarán el desarrollo del producto y limitarán sus características, y el mercado no los recompensará.

Peor aún, las empresas tienen importantes alicientes para tratar los problemas de seguridad como si fueran problemas de relaciones públicas, por lo que se guardan el conocimiento sobre las vulnerabilidades de seguridad y los compromisos de datos para sí mismas. Equifax se enteró de su hackeo de 2017 en julio, pero logró mantenerlo en secreto hasta septiembre;[13] cuando piratearon Yahoo en 2014, la empresa no dijo nada hasta dos años después,[14] y Uber tardó un año.[15]

Aunque esta información se haga pública, no es suficiente. A pesar de la mala prensa, las indagaciones del Congreso y la indignación en las redes sociales, las empresas, por lo general, no suelen ser castigadas en el mercado por su mala seguridad. Un estudio descubrió que los precios de las acciones de las compañías vulneradas no se ven afectados a largo plazo.[16]

Ya hemos visto antes las consecuencias de los incentivos mal alineados. En los años previos a la crisis financiera de 2008, los banqueros en realidad estaban jugando con el dinero de otras personas. Les interesaba obtener todas las ganancias posibles a corto plazo, pero no tenían ningún estímulo que les hiciera pensar en las consecuencias para las familias que invertían todos sus ahorros en productos de riesgo. La mayoría de los consumidores no tuvieron más remedio que confiar en el consejo de sus banqueros, porque no eran expertos financieros y no podían evaluar los riesgos. Después de la crisis, el Congreso introdujo la ley Dodd-Frank para realinear los incentivos. Ahora los banqueros se enfrentan a mayores deberes legales (por ejemplo, primero deben considerar si un consumidor podría pagar un préstamo antes de otorgarlo) y han aumentado las sanciones por mala praxis.

Aproximadamente el 90 % de la infraestructura de Internet es privada.[17] Entre otras cosas, esto significa que se gestiona para optimizar los intereses financieros a corto plazo de las empresas que pueden influir en él, no los intereses de los usuarios o la seguridad general de la red.

Necesitamos cambiar los incentivos para que las empresas se vean obligadas a preocuparse por las implicaciones de seguridad de sus productos.

Una manera de hacerlo es multar a las compañías (y a sus directores) cuando hagan mal las cosas. Estas multas deben ser lo bastante grandes como para cambiar la ecuación de riesgo de la compañía. El coste de la inseguridad, por lo general, se calcula como la amenaza multiplicada por la vulnerabilidad multiplicada por las consecuencias. Si el resultado no es menor que el coste de reducir el riesgo, una compañía razonable asume el riesgo. Las multas, ya se evalúen después de un incidente o mediante una sanción por prácticas inseguras, elevan el coste de la inseguridad y hacen que el pago de la seguridad sea mucho más atractivo financieramente.

En algunos casos, las multas pueden llevar a las empresas a la bancarrota. Es algo grave, pero es la única forma de demostrarle al resto de la industria que nos tomamos en serio la ciberseguridad. Si una persona mata a tu cónyuge, la enviarán a la cárcel y podría incluso ser castigada con la pena de muerte. Si una empresa mata a tu cónyuge, debería enfrentarse al mismo destino. El autor John Greer propone enviar a las empresas convictas a una pseudocárcel: serían arrestadas por el Gobierno, se desharían de todos los inversores y luego se venderían.[18] Si tememos imponer la pena de muerte a las empresas, estas se darán cuenta de que pueden escatimar en seguridad y contar con la misericordia de la sociedad.

Otra forma de pensar acerca de esto es que, si una empresa solo puede mantenerse en el negocio mediante la externalización del coste de la seguridad, entonces tal vez no debería estar en él. Estas compañías no le piden a la sociedad que pague los salarios de sus empleados, ¿por qué deberíamos entonces pagar por sus fallos de seguridad? Es como una fábrica que solo puede permanecer en el negocio contaminando ilegalmente; todos estaríamos mejor si la cerraran.

Piensa en profesiones reguladas, como el derecho y la contabilidad. Las empresas que se especializan en estos servicios profesionales se toman en serio sus responsabilidades legales, en parte porque las consecuencias pueden ser terribles. Sería muy difícil encontrar un socio en una firma de auditorías al que el hundimiento de Arthur Andersen no le parezca tan importante. Arthur Andersen era una de las cinco firmas de contabilidad global más importantes y tenía más de 85.000 empleados que más o menos desaparecieron de la noche a la mañana después de que la acusaran de haber auditado indebidamente las cuentas financieras de Enron (un delito de regulación muy serio y grave).[19]

Y este fracaso ilustra otro punto. Los empleados de Arthur Andersen lo hicieron bien, ya que otras compañías adquirieron las diferentes partes. Una empresa similar que se haya quedado fuera del negocio debido a prácticas de seguridad negligentes también haría que adquiriesen sus departamentos otras compañías, ojalá más diligentes.

Pero incluso esto no es suficiente. En particular, las empresas emergentes ignorarían racionalmente la seguridad y se arriesgarían a que las multaran o incluso a ir a la pseudocárcel. Ya están arriesgando mucho más con mucho menos, y saben que el éxito depende tanto de la suerte como de las habilidades empresariales. Sería inteligente que usaran su tiempo y su presupuesto limitados para crecer más rápido, arriesgarse y preocuparse por la seguridad más adelante. Sus inversores y miembros de la junta también lo recomendarían.

En 2015, Volkswagen fue sorprendida haciendo trampas en sus pruebas de control de emisiones. Debido a que el software controla el funcionamiento del motor, los programadores crearon un algoritmo que detectaba cuándo se estaba realizando una prueba de emisiones y como respuesta modificaba el comportamiento del motor.[20] ¿El resultado? De 2009 a 2015, once millones de vehículos en todo el mundo (500.000 en Estados Unidos) emitieron hasta cuarenta veces más contaminantes de lo que permitían las leyes locales. La compañía recibió multas y sanciones por un total de casi 30.000 millones, y

eso es significativo.[21] Pero mi miedo es que la gran lección del caso de Volkswagen no es que, si una empresa hace trampas, la van a descubrir, sino que es posible hacer trampas durante seis años; un período más prolongado que el tiempo que están en el cargo la mayoría de los directores ejecutivos, quienes esperaban cobrar mucho antes de que llegaran las grandes multas. (Nota: un directivo de VW y un ingeniero fueron condenados a prisión por sus actos)[22].

Sin duda, este es solo uno de los aspectos de un problema mucho mayor sobre los incentivos dentro de las empresas. La única forma de motivarlas es responsabilizar personalmente a los ejecutivos y a los miembros de la junta directiva (incluidos los inversores de capital riesgo, quienes suelen formar parte de las juntas directivas de las empresas en las que invierten) por los fallos en la seguridad, lo que aumentará los costes personales de la inseguridad y hará menos probable que esas personas se salgan con la suya para obtener beneficios.

Esta rendición de cuentas puede llegar pronto. Conforme a la ley actual en Estados Unidos y el RGPD (Reglamento General de Protección de Datos) de la UE, los ejecutivos y miembros de la junta directiva podrían enfrentarse a responsabilidades por filtraciones de datos.[23] Y la fuerza de las expectativas de la sociedad también se está moviendo en esta dirección. Los directores ejecutivos, responsables de sistemas de información y directores de investigación de Equifax se vieron obligados a retirarse anticipadamente a raíz de este ataque. En el Reino Unido, el CEO de TalkTalk renunció después de que multaran a la empresa con 400.000 libras esterlinas por divulgar los datos de sus clientes.[24]

Existe un precedente para responsabilizar a estas personas. La Ley Sarbanes-Oxley regula la conducta financiera corporativa y la mala conducta. Se aprobó en 2002 como respuesta a los delitos y abusos de Enron para rectificar los numerosos conflictos de intereses que socavaron la efectividad de muchas leyes corporativas. Según la Sarbanes-Oxley, los directores pueden responder personalmente por el comportamiento de su empresa, lo que debería motivarlos a no permitir que las compañías hagan nada ilegal.[25] La realidad de la ley podría estar por debajo de sus expectativas,[26] pero es la idea adecuada. Tenemos que pensar en hacer lo mismo con la seguridad del software.[27]

No voy a fingir que cambiar la responsabilidad de las obligaciones no sea una gran batalla. Es difícil aumentar las responsabilidades donde no se requieren, porque supone un cambio radical para las industrias afectadas, que

lucharán en cada paso del camino, aunque no hacerlo sería algo peor para la sociedad.

Por último, mejorar los incentivos no tiene que tratarse solo de imponer sanciones por hacer las cosas mal. Es más probable que las compañías estén dispuestas a divulgar públicamente información sobre fallos de seguridad si reciben algún tipo de exención de responsabilidades. También podrían inclinarse más a informar sobre vulnerabilidades a competidores o al Gobierno si tienen garantías de que su propiedad intelectual sensible quedará protegida. Y los créditos fiscales también tienen su importancia.

DETERMINAR RESPONSABILIDADES

Las multas de los organismos gubernamentales no son la única forma de inclinar a Internet+ hacia la seguridad. El Gobierno puede cambiar la ley para facilitar que los usuarios demanden a las empresas cuando falla su seguridad.

SmartThings es una plataforma centralizada que funciona con bombillas compatibles, candados, termostatos, cámaras, timbres y demás controlados por una aplicación de teléfono gratuita. En 2016, un grupo de investigadores encontró una gran cantidad de brechas de seguridad en el sistema; fueron capaces de robar los códigos que abrirían las puertas, dispararían una falsa alarma de incendio y deshabilitarían algunas configuraciones de seguridad.[28]

Si una de esas vulnerabilidades permitiera que un ladrón irrumpiera en tu hogar, ¿de quién sería el problema? Tuyo, por supuesto. Si leías las condiciones de uso de SmartThings, quedaba claro que utilizarías sus productos bajo tu propia cuenta y riesgo, bajo ninguna circunstancia la empresa se haría responsable de ningún daño en caso de fallo o mal funcionamiento y aceptarías que SmartThings no respondiera por ningún daño ni ante ninguna reclamación.[29]

Desde el comienzo de los ordenadores personales, tanto los fabricantes de hardware como los de software renunciaron a sus responsabilidades cuando las cosas salían mal. Esto tenía algún sentido durante los primeros años de la informática. La razón por la que tenemos Internet es porque las empresas pudieron comercializar productos chapuceros. Si los ordenadores estuvieran sujetos a las mismas regulaciones de responsabilidad de producto que las escaleras, es probable que todavía no estuvieran disponibles en el mercado.

Parte de esta desigualdad se aplica a las condiciones de uso que rigen la relación de responsabilidad que tienes con la compañía cuyo software utilizas. Estos son los términos y condiciones de uso que debes confirmar que has

leído, aunque nadie lo hace nunca.[30] No es que importe que los leas: las empresas se reservan el derecho a modificar las condiciones a voluntad sin avisarte.[31]

Las empresas no son responsables si sus programas pierden tus datos, los exponen a delincuentes o causan daños, ni tampoco los servicios en la nube. Los términos y condiciones de uso, más o menos, te obligan a asumir todos los riesgos al utilizar los productos y servicios, y protegen a las empresas de los juicios cuando surgen problemas.

Demandar a los proveedores de software también es caro. La mayoría de los usuarios no pueden hacerlo solos, necesitan demandas colectivas. Para prevenir esto, muchos términos y condiciones de uso incluyen acuerdos de arbitraje vinculantes, lo que obliga a los usuarios descontentos a pagar el arbitraje, que por lo general es mucho más favorable para las empresas que un tribunal.[32] Prevenir las demandas colectivas también privilegia mucho a las empresas.

Todo esto se agrava por la exención del software de la ley ordinaria de responsabilidad de producto. Según los estándares internacionales, Estados Unidos tiene leyes de responsabilidad de producto bastante estrictas, pero solo cuando se trata de productos tangibles. Los usuarios de productos tangibles defectuosos pueden demandar a cualquiera en la cadena de distribución, desde el fabricante hasta el minorista que lo vendió. El software logra evadir todo esto, tanto porque a menudo se licencia en lugar de comprarse como porque el código está categorizado legalmente como un servicio, en lugar de como un producto. E incluso cuando se trata de un producto, el fabricante puede renunciar a la responsabilidad en el acuerdo de la licencia del usuario final, algo que los tribunales han confirmado.

Hay otros dos grandes problemas.

Primero, cuando el software defectuoso ha provocado pérdidas, los tribunales se han mostrado reacios a aceptar que las compañías de software *hayan causado* ese daño. Los jueces tienden a culpar a los hackers por explotar vulnerabilidades, no a las empresas por crear la posibilidad en primer lugar.[33] La necesidad de evidencias complica esto aún más. Si vives en Estados Unidos, casi seguro que fuiste víctima de la filtración de Equifax. Pero, si tu información se utiliza para cometer fraudes y robo de identidad, no podrás probar que el hackeo de Equifax fue el verdadero culpable. Es probable que te hayan robado información en múltiples ocasiones desde numerosas bases de datos. Esta es la razón por la que es tan difícil demandar a empresas como Equifax cuando pierden tus datos personales: todos los datos

que la empresa no pudo obtener ya están disponibles en el mercado negro, por lo que una filtración más no va a causar daños nuevos.[34]

Después de que la red zombi Mirai causara el mayor ataque DDoS en la historia de Estados Unidos, la Comisión Federal de Comercio (FTC, por sus siglas en inglés) intentó responsabilizar a los fabricantes de rúters D-Link, pero no pudo. No pudieron probar que se usaran rúters individuales como parte de la red de robots Mirai, solo que los rúters D-Link eran inseguros y que algunos de ellos se utilizaban con este fin.[35]

En segundo lugar, los usuarios luchan constantemente por demostrar que han sufrido *daños*, según la definición que hace la ley de este término. Los tribunales solo oirán casos de este tipo en los que haya denuncias por daños monetarios, lo cual es muy difícil de demostrar para violaciones de la privacidad.

En 2016, la FTC publicó que LabMD había participado en prácticas desleales al no proteger la información confidencial de sus clientes. La FTC descubrió que LabMD no había implementado ni siquiera las medidas básicas de seguridad de datos, y había dejado la información médica y financiera confidencial expuesta durante casi un año.[36] LabMD impugnó la decisión de la FTC en el Tribunal de Apelaciones argumentando que, dado que no había casos conocidos de que los datos expuestos se hubieran utilizado con fines ilícitos, sus clientes no habían sido perjudicados por su laxa seguridad y la FTC no tenía autoridad para sancionarlos. Todo parece indicar que el Tribunal decidirá a favor de LabMD,[37] una decisión que obstaculizará la capacidad futura del organismo para penalizar a las organizaciones que violen la privacidad de sus clientes.

En el capítulo 1 mencioné a la compañía de cerraduras electrónicas Onity, cuyos bloqueos de puertas en las principales cadenas hoteleras fueron pirateados para permitir robos. La demanda colectiva de 2014 de las cadenas hoteleras se desestimó porque las cerraduras aún funcionaban y los demandantes no podían señalar estos robos como resultado del fallo de seguridad.[38]

La ley de responsabilidad no tiene que funcionar de esta manera. Basta con mirar el historial de responsabilidad de producto para las manufacturas. Después de la Revolución Industrial, la ley utilizó al principio la rigurosa cláusula *caveat emptor*: que el comprador tenga cuidado; sin embargo, a medida que las manufacturas se industrializaban y los productos se volvían más complejos, los tribunales y los legisladores reconocieron poco a poco que no era razonable esperar que los consumidores evaluaran la seguridad de los

productos que compraban. Desde finales de 1800, las leyes de responsabilidad de producto surgieron de manera gradual. Luego, a partir de mediados de siglo la mayoría de las economías industriales pasaron a tener estándares de responsabilidad estricta. Si un producto causa daños físicos, los fabricantes son responsables, incluso aunque no fueran negligentes haciendo el producto defectuoso. En la década de los cuarenta, la Corte Suprema de California explicó de manera ya famosa por qué la estricta responsabilidad de los productos manufacturados tenía sentido: «La política pública exige que la responsabilidad se fije donde reduzca más eficazmente los riesgos para la vida y la salud inherentes a los productos defectuosos que llegan al mercado».[39] Un argumento que también se aplica a Internet+.

Además, las personas no deberían tener que demostrar que han sufrido perjuicios monetarios para poder responsabilizar a los proveedores de software por unos productos defectuosos que eran evitables. La ley podría prever indemnizaciones en caso de que la seguridad de las empresas fuera ineficaz para los dispositivos que venden, los servicios que proporcionan o los datos que guardan. Las indemnizaciones tendrán lugar una vez que se demuestre una seguridad deficiente, sin requisitos adicionales de daños económicos. Así funciona la ley de interceptaciones telefónicas: si se demuestra que un departamento de policía ha escuchado a alguien de forma ilegal, tendrá que pagar una indemnización.[40] Esta es también la forma en que funciona la ley de derechos de autor: un infractor tiene que pagar daños al titular de los derechos, incluso aunque no haya habido ningún daño económico.[41] Obviamente, esto no servirá para todas las áreas de seguridad de Internet+, pero sí para algunas.

Creo que todos estos tipos de argumentos ganarán terreno en relación con Internet+. En este momento, las agencias reguladoras están considerando temas de privacidad de datos y de seguridad informática, y muchos de los productos que se están informatizando y conectando ya están sujetos a las leyes de responsabilidad civil: automóviles, dispositivos médicos, electrodomésticos, juguetes, etc. Cuando las versiones conectadas de estos objetos empiecen a matar gente, los tribunales tomarán medidas y la sociedad exigirá un cambio legislativo.[42]

Sin embargo, los softwares que tenemos hoy en día están todavía en la Edad Oscura de la responsabilidad del producto. Cuando las cosas van mal, por lo general la pérdida debe asumirla el usuario; las empresas más o menos se libran de la seguridad.

La responsabilidad no tiene por qué ahogar la innovación. Los incentivos no pretenden ser un medio de intervención gubernamental o blanco o negro, o todo o nada. En general, la ley establece exenciones de responsabilidad en algunas circunstancias, como sucedió en la década de los ochenta, cuando la industria de los pequeños aviones estaba casi en bancarrota debido a excesivos juicios de responsabilidad.[43] También podrían establecerse límites para los daños, como en el caso de algunas reclamaciones por negligencias médicas, aunque debemos tener cuidado de que estos límites no mermen la responsabilidad. Y, aunque está claro que los fabricantes de software no merecen ser responsables al cien por cien de un fallo de seguridad, tampoco merecen no serlo en absoluto. Los tribunales deben resolver esta cuestión.

Donde hay riesgos de responsabilidad, aparece la industria de los seguros.[44] Un mercado de seguros que funcione de manera adecuada protegerá a las compañías de que las fuercen a abandonar el negocio por reclamaciones de responsabilidad: las hace ser conscientes de que el riesgo de que sus productos causen daños a los usuarios es el precio normal de hacer negocios.

Los seguros también son un mecanismo de autorreforzamiento para mejorar la seguridad y la protección, al tiempo que les permite a las empresas innovar. La industria de seguros impone costes a la mala seguridad. Una empresa cuyos productos y servicios se muestren vulnerables se enfrentará a primas más altas, lo que la motivará a gastar dinero para mejorar su seguridad y reducir esas primas. Por otro lado, si hackean de todas formas a una empresa adherida a estándares razonables, esta estará protegida en un juicio importante porque su compañía de seguros correrá con las costas.

Los seguros también funcionan de forma individual. Si exigimos que las personas que compran tecnologías peligrosas también paguen por un seguro, entonces estamos privatizando en la práctica la regulación de estas tecnologías.[45] El mercado determinará cuánto costará ese seguro, dependiendo de la seguridad de las tecnologías. Los fabricantes podrían hacer que sus productos tuvieran seguros baratos aumentando la seguridad, aunque, en cualquier caso, los consumidores pagarán el riesgo inherente a lo que compran.

Existen desafíos a la hora de crear estos nuevos productos de seguros. Hay dos modelos básicos para los seguros: el modelo de incendios, que determina que las casas individuales se incendian según una tasa bastante constante, y la industria de seguros puede calcular las primas en función de esa tasa, y el modelo de inundación, en el que un evento poco frecuente a gran escala afecta a un gran número de personas, pero también a un ritmo constante. El

seguro de Internet+ es complicado porque no sigue ninguno de estos modelos, sino que tiene aspectos de ambos: los individuos son pirateados según una tasa constante (si bien en aumento), mientras que las roturas de clase y las violaciones masivas de datos afectan a muchas personas a la vez. Además, el panorama tecnológico en constante cambio hace que sea difícil recopilar y analizar los datos históricos necesarios para calcular las primas. Tal vez sea más adecuado utilizar el modelo de los seguros de salud: la enfermedad es inevitable y los contagios pueden extenderse ampliamente, por lo que las aseguradoras deberían centrarse en la prevención de riesgos y la respuesta a incidentes en lugar de en reembolsos directos.[46] Sin embargo, en algunos casos, las compañías de seguros están empezando a averiguar cómo asignar precios a las primas de los seguros de ciberseguridad clasificando a las empresas según sus prácticas en materia de seguridad.[47] Cuando aclaremos las responsabilidades, ocurrirán más cosas.

CORREGIR ASIMETRÍAS INFORMATIVAS

Hace poco, tuve la ocasión de investigar monitores para bebés. Por su diseño se corresponden con dispositivos de vigilancia y pueden captar mucho más que los llantos de un bebé. Por supuesto, tuve muchas preguntas respecto a la seguridad.[48] ¿Cómo se protege la transmisión de audio y vídeo? ¿Cuál es el algoritmo de cifrado? ¿Cómo se generan las claves de cifrado y quién tiene copias de ellas? Si los datos se almacenan en la nube, ¿durante cuánto tiempo y cómo se protegen? ¿Cómo se autentica la aplicación de teléfonos inteligentes, si el monitor utiliza una, en el servidor de la nube? Muchas marcas son hackeables y yo quería comprar una segura.[49]

El material de marketing del producto apenas informa. Los monitores analógicos no dicen nada sobre seguridad. Los digitales hacen declaraciones vagas como esta: «[Nuestra] tecnología transmite una señal segura y encriptada para que pueda estar seguro de que usted es el único que puede escuchar a su bebé».[50] Algunos afirman seguir varios estándares inalámbricos, y unen al remitente y al receptor mediante algún tipo de cifrado. Otros dependen por completo de la potencia de transmisión y el cambio de canal para la seguridad. Todos juegan con la palabra *seguro* sin explicar lo que esto significa. Básicamente, la comparativa entre productos es imposible. No puedo distinguir lo bueno de lo malo, y esto significa que el consumidor promedio no tiene ninguna oportunidad de hacerlo.[51]

La seguridad es compleja y en gran parte opaca, y en este momento no hay manera de que los usuarios distingan los productos seguros de los inseguros. Los monitores para bebés son bastante simples. El problema de los dispositivos del IoT se complicará aún más a medida que los dispositivos (y las interconexiones entre ellos) se vuelvan más complejos. La falta de información combinada con la complejidad de los sistemas está quitándole poder al consumidor, y casi con toda seguridad lo induce a pensar que los dispositivos son más seguros de lo que en realidad son.

En economía, esto se conoce como *mercado de limones*.[52] Los proveedores solo compiten por las características que los compradores pueden percibir e ignoran las que no, como la seguridad. Las afirmaciones vagas y tranquilizadoras sobre las características de la seguridad tienen más probabilidades de dar como resultado una venta que unas explicaciones muy detalladas.

El resultado es que los productos inseguros sacan del mercado a los seguros, pues no hay retorno en la inversión en seguridad.[53] Lo hemos visto una y otra vez en la seguridad informática y de Internet, y también lo veremos en Internet+. La seguridad debe ser significativa, vívida y obvia para el consumidor; cuando los consumidores sepan más, estarán capacitados para tomar mejores decisiones.

Muchas industrias tienen requisitos de etiquetado. Piensa en la nutrición y las etiquetas de los ingredientes de los alimentos, toda la letra pequeña que acompaña a los productos farmacéuticos, las etiquetas de eficiencia de combustible en los coches nuevos, etc. Este etiquetado les permite a los consumidores tomar mejores decisiones de compra. Hoy en día no existe nada parecido en la seguridad informática.[54]

Un requisito de etiquetado útil para productos informatizados sería un análisis sobre el modelo de amenazas a las que el dispositivo puede responder. Fijándonos de nuevo en el monitor del bebé, el cambio aleatorio de canales podría frustrar a un interceptor ocasional, pero no a un atacante más sofisticado. Otras medidas de seguridad serían más efectivas que el cambio de canal. Si el fabricante explica la seguridad de una manera simple, los consumidores pueden hacer más comparaciones en sus compras. Estoy pensando en afirmaciones como: «Este monitor para bebés empareja de forma única los transmisores y los receptores entre sí», «Las transmisiones están cifradas entre el transmisor y el receptor, lo que protege contra las escuchas no deseadas», «Las transmisiones en tu red inalámbrica están cifradas, lo que las asegura contra las escuchas no deseadas de la red» o «Este producto

encripta el audio y el vídeo enviado a la nube, lo que lo protege contra las escuchas no deseadas en Internet». Y aunque gran parte de esto pueda parecer una jerigonza para el consumidor promedio, los sitios de reseñas de productos pueden utilizar esta información para dar mejores recomendaciones.

Samsung hizo algo así con su televisión inteligente, pero quedó sepultado por la letra pequeña de sus políticas:

> Tenga en cuenta que si las palabras que pronuncia incluyen información personal o sensible, esa información quedará entre los datos transmitidos a un tercero a través del uso de la función de reconocimiento de voz.[55]

Las etiquetas de los productos también deben explicar las responsabilidades de seguridad del usuario. Los monitores de bebé suelen colocarse en habitaciones. Es mucho más fácil dejar un monitor encendido todo el tiempo que encenderlo y apagarlo, lo que significa que es muy probable que capture y transmita la actividad que el usuario no desea transmitir. Quiero que el producto avise al usuario de que esto sucederá. «Cuando el transmisor está encendido, transmite todos los sonidos que captura a nuestra sede en San José» o «Este producto deberá actualizarse periódicamente, los usuarios registrados recibirán actualizaciones por lo menos durante los próximos cinco años». La idea general es que los usuarios estén informados de dónde comienzan y terminan las características de seguridad del producto, cómo se debe mantener la seguridad y cuándo los usuarios siguen por su cuenta y riesgo.

Quizá la forma más útil de dar información a los clientes en las etiquetas de los productos sea un sistema de calificación. Los productos y servicios seguros pueden obtener una puntuación más alta, un sello de seguridad o alguna otra marca simple que guíe las decisiones de compra de los clientes. Es una idea interesante, y muchos organismos gubernamentales están pensando en ello: en el Reino Unido,[56] la UE,[57] Australia[58] y en otros lugares.

Necesitamos más transparencia en los servicios en la nube. En este momento no tienes idea de cómo Google protege tu correo electrónico. Espero que las obligaciones de las empresas cambien esto. Si una empresa minorista es responsable de proteger los datos de sus clientes, tendrá que responsabilizar también a sus proveedores de servicios en la nube de ello. Y esos proveedores de servicios, a su vez, tendrán que responsabilizar a sus proveedores de infraestructura en la nube. Este tipo de responsabilidad en

cascada obligará a todos a ser más transparentes, aunque solo sea para satisfacer las demandas de las compañías de seguros.

Si existen estándares de seguridad, un organismo gubernamental o una organización independiente podría probar productos y servicios para asignarles calificaciones. Los informes propios también podrían funcionar. En 2017, dos senadores presentaron la Ley Ciberescudo, dirigida al Departamento de Comercio para desarrollar estándares de seguridad en dispositivos IoT. Trataba de que las empresas mostraran una etiqueta en sus productos indicando su adhesión a los estándares.[59] El proyecto de ley no llegó a ninguna parte, pero un consorcio industrial o un tercero podría hacer lo mismo con facilidad. Los estándares podrían incluso vincularse con los seguros.

De forma alternativa, las empresas pueden calificarse en función de sus procesos y prácticas, quizá utilizando los principios de diseño del capítulo 6. Algo parecido a lo que hacen los laboratorios Underwriters, un grupo creado por la industria de seguros en 1894 para probar la seguridad de los equipos eléctricos; no demuestran que un producto sea seguro, pero usan una lista de verificación para confirmar que el fabricante haya seguido un conjunto de reglas de seguridad.

La Unión de Consumidores (la organización detrás de los *Informes del Consumidor*) ha tratado de hacer algún tipo de prueba de seguridad a los productos de IoT durante años. Incluso podría tener ya un sistema de calificación viable para cuando se publique este libro.[60] Pero, si bien puede calificar los automóviles y los principales electrodomésticos, la cantidad de dispositivos de consumo más baratos que hay (y los rápidos cambios) complican que cualquier organización de propósito general pueda lidiar con ello.

En el campo de la seguridad informática vale la pena mencionar dos programas de calificación existentes. El Proyecto ¿Quién te Cubre la Espalda? de Electronic Frontier Foundation evalúa los compromisos de las empresas para proteger a los usuarios cuando el Gobierno busca datos privados.[61] Y la iniciativa de evaluar los derechos digitales de Open Technology Institute evalúa si las empresas respetan la libertad de expresión y la privacidad.[62]

Sin embargo, cuando se trata de productos, habrá algunos obstáculos en la configuración de un sistema de clasificación de seguridad. Uno es que no existen pruebas simples con resultados simples. No podemos probar a fondo un software y declararlo seguro, y cualquier calificación de seguridad cambia con el tiempo: lo que era verificable y seguro el año pasado podría ser

inseguro este año. Esto es más que una cuestión de tiempo y de gastos. Estamos enfrentándonos a los límites tecnológicos de las ciencias de computación: nuestra incapacidad para certificar algo como seguro de manera significativa.

Aun así, todavía hay mucho que podemos hacer: podemos probar la resistencia de un producto a un conjunto conocido de técnicas de ataque, probarlo en busca de comportamientos indicativos de errores de seguridad y demostrar un proceso de desarrollo de unidades defectuosas o probar muchos de los principios de diseño del capítulo 6; y podemos hacer muchas de estas cosas sin el consentimiento de las compañías que desarrollan y venden el software.[63]

Tendremos que encontrar el equilibrio adecuado entre los requisitos de prueba factibles y la seguridad. Por ejemplo, la Administración de Alimentos y Medicamentos estadounidense (FDA, por sus siglas en inglés) requiere pruebas de los dispositivos médicos informatizados. En sus inicios, sus reglas exigían una nueva prueba completa si había algún cambio en el software, incluidos parches para corregir vulnerabilidades, pero se ha revisado para que las actualizaciones que no cambian la funcionalidad no requieran de una nueva prueba. No es la forma más segura de hacer las cosas, pero tal vez sea el compromiso más razonable.

También tendremos que descubrir cómo educar a los clientes para que comprendan el significado de las calificaciones, clasificaciones, descripciones o sellos de aprobación. ¿Cómo explicamos que un logotipo que indica que un juguete del IoT cumple con los estándares de seguridad de la industria A-1 no quiere decir que se garantice que el juguete sea seguro, solo que cumple con unos estándares de seguridad mínimos que pueden ser lo suficientemente buenos hoy en día contra ciertas amenazas? En el mundo de la alimentación hay un millón de clasificaciones y escalas; no queremos que eso suceda con la seguridad de Internet+.

A pesar de estos problemas, será esencial algún tipo de calificación de seguridad. No soy capaz de imaginar cualquier mejora de seguridad basada en el mercado sin ella.

Más allá del etiquetado de productos y las clasificaciones de seguridad, hay otras dos buenas maneras de darles a los consumidores más información. La primera son las leyes de divulgación por incumplimiento, que requieren que las empresas informen a las personas si les han robado su información personal. Esto no solo alerta a la gente acerca de que sus datos han sido robados, sino que también nos ofrece información sobre las prácticas de

seguridad de las compañías que almacenan datos personales. En Estados Unidos, 48 estados tienen este tipo de leyes,[64] aunque todas son diferentes: qué información cuenta como personal, cuánto tiempo tienen las empresas para divulgarla, cuándo pueden retrasar esta divulgación, etc.

Ha habido varios intentos fallidos de tener una ley nacional.[65] En teoría, estoy a favor de ello, aunque me preocupa que sea menos exhaustiva que otras leyes estatales, en especial en Massachusetts, California y Nueva York, y que adelante a todas las leyes estatales existentes. En este momento, las leyes estatales son leyes nacionales *de facto*, porque cada gran empresa tiene clientes en los cincuenta estados.

Hay que ampliar estas leyes estatales. La notificación de incidentes en los que no se pierde información personal sigue siendo voluntaria, y la participación suele ser baja porque las empresas temen la mala prensa o los litigios. Las leyes de divulgación de infracciones también deben abarcar otro tipo de faltas. Si se viola una parte de la infraestructura crítica, por ejemplo, debería existir un requisito para que el propietario informe sobre ello.

La segunda forma de proporcionar más información a los consumidores es mejorar la divulgación de vulnerabilidades. En el capítulo 2 hablaba sobre cómo los investigadores de seguridad encuentran puntos débiles en los programas informáticos y sobre cómo la publicación de los resultados de esas investigaciones es fundamental para motivar a los proveedores de software a solucionarlos. Los proveedores odian el proceso porque les da mala imagen, y en algunos casos han demandado con éxito a investigadores amparándose en la Ley de Derechos de Autor de la Era Digital y otras. Hay que revertir esta situación; lo que necesitamos son leyes que protejan a los investigadores que encuentren vulnerabilidades, las divulguen de manera responsable al proveedor de software y publiquen sus resultados después de un tiempo razonable. No solo la mejorada divulgación de vulnerabilidades ayudará a las empresas a aumentar su seguridad y a evitar una publicidad desfavorable,[66] sino que también les dará a los consumidores información importante sobre la seguridad de los diferentes productos.

AUMENTAR LA EDUCACIÓN PÚBLICA

La educación pública es vital para la seguridad de Internet+. Los ciudadanos deben entender su papel dentro de la ciberseguridad: como cualquier otro aspecto de la seguridad personal o pública, nuestras acciones individuales son importantes. Además, las personas bien informadas podrán forzar a las

empresas a que mejoren su seguridad, ya sea rechazando el uso de productos o servicios inseguros o presionando al Gobierno para que tome medidas cuando sea apropiado.

Ha habido algunos intentos de hacer campañas de sensibilización pública sobre la seguridad en Internet. El Departamento de Seguridad Nacional estadounidense dio a conocer la campaña Para.Piensa.Conecta en 2016.[67] El hecho de que con toda probabilidad no estés familiarizado con ella demuestra lo eficaz que ha sido. Quizá otras campañas puedan hacerlo mejor.

La educación es difícil. Necesitamos educar a las personas sobre la importancia de la seguridad y acerca de cómo tomar decisiones sobre ella sin convertirlas en ingenieros especializados. Se trata de problemas técnicos, pero no queremos crear un mundo donde solo los expertos tengan garantizada la seguridad. Y ahí es donde nos encontramos ahora con nuestros ordenadores portátiles y nuestras redes domésticas. La complejidad de estos sistemas va más allá de la comprensión del consumidor promedio. Tienes que ser un experto para configurarlos, por lo que la mayoría de la gente ni se molesta. Tenemos que hacerlo mejor.

Hoy en día, una gran cantidad de los consejos de seguridad que les damos a los usuarios solo abarca el mal diseño de seguridad.[68] Les decimos que no hagan clic en enlaces extraños, pero es Internet, y hacer clic es para lo que sirven los enlaces. También les decimos que no inserten unidades USB extrañas en su ordenador. Otra vez lo mismo, ¿qué otra cosa podrías hacer con una unidad USB? Tenemos que hacerlo mejor: necesitamos sistemas que sean seguros sin importar en qué enlaces haga clic la gente y sin importar qué unidades USB inserten en sus ordenadores.

Compara esto con el automóvil. Cuando los coches se presentaron por primera vez se vendían con un manual de reparación y un juego de herramientas: era necesario saber cómo arreglar uno para poder conducirlo. A medida que los coches eran más fáciles de usar y las estaciones de servicio más comunes, incluso los que eran reacios a la mecánica podían comprar uno. Hemos llegado a este punto con los ordenadores, pero no con la seguridad informática.

Por otro lado, hay áreas donde la educación pública no ayuda. Para aparatos de bajo coste no hay una solución de mercado porque la amenaza proviene sobre todo de redes de robots, y ni el comprador ni el vendedor saben lo suficiente sobre ellas como para preocuparse (excepto personas como yo y quizá algunos de mis lectores). Los propietarios de las cámaras web y los DVR utilizados en los ataques de denegación de servicio no pueden

decirlo, y a la mayoría no les importa: sus dispositivos fueron baratos, todavía funcionan y no conocen a ninguna víctima. A los vendedores de esos dispositivos tampoco les importa: ahora están vendiendo modelos más nuevos y mejores, y sus clientes solo se preocupan por el precio y las características. Piensa en ello como una especie de contaminación invisible.

El mercado funciona mejor con artefactos más caros y a medida que aumentan los riesgos de seguridad. Los conductores de automóviles y los pasajeros de las aerolíneas quieren que esos aparatos sean seguros. En realidad, la educación podría ayudar a las personas a tomar mejores decisiones sobre la seguridad de sus productos, tal como lo hacen hoy sobre la seguridad de sus automóviles.

Podemos enseñarles a los usuarios comportamientos específicos, siempre que sean simples, prácticos y tengan un sentido obvio. En lo referente a salud pública les hemos enseñado a las personas que deben lavarse las manos, taparse cuando estornudan y vacunarse contra la gripe cada año. Menos personas de las que quisiéramos hacen esas cosas, pero la mayoría sabe que debería hacerlo.

ELEVAR LOS ESTÁNDARES PROFESIONALES

Hay muchas reglas que debes seguir si quieres construir un edificio: necesitas contratar a un arquitecto para diseñarlo que esté colegiado; cualquier ingeniería complicada debe aprobarla un ingeniero autorizado; la empresa de construcción debe tener una licencia, y todos los electricistas y aprendices que esta contrata deben estar cualificados por organismos estatales; para navegar por las complejidades de todo esto, seguramente necesites contratar un abogado y un contable, ambos acreditados y autorizados por el Estado, y, por supuesto, el agente inmobiliario que te ayudó a comprar el terreno también tendrá su licencia o estará inscrito en algún registro, en función del lugar.

En algunos países, la certificación profesional es un estándar más alto que las licencias ocupacionales, pero en este momento no hay ningún sistema para certificar o licenciar a los diseñadores de software, arquitectos de software, ingenieros informáticos o programadores de ninguna clase. Crearlo no es una idea nueva, se ha promovido en la industria durante décadas. Las organizaciones existentes para profesionales de software, como el Instituto de Ingeniería Eléctrica y Electrónica (IEEE, por sus siglas en inglés), han estudiado este tema con detenimiento y han propuesto varios esquemas de licencias y criterios de desarrollo profesional diferentes para los ingenieros de

software.[69] La Organización Internacional de Normalización (ISO, por sus siglas en inglés) también tiene algunos estándares relevantes.[70] Siempre ha habido un fuerte rechazo por parte de los desarrolladores, tanto por razones personales como porque la ingeniería de software no es ingeniería en el sentido tradicional. No es una disciplina donde el ingeniero aplique principios conocidos basados en la ciencia para crear algo nuevo. Esto hace que sea difícil descubrir qué es un ingeniero de software profesional, y mucho menos qué competencias requiere su trabajo.

Aun así, creo que esto va a cambiar. Habrá algún tipo de ingeniero de software que tenga licencia, ya sea por parte del Gobierno o por alguna asociación profesional con la aprobación de este, y se le solicitará que firme el diseño del software de la misma forma que hace un arquitecto colegiado con los planes de construcción.

Sin embargo, se necesitará mucho trabajo para conseguirlo. No puedes crear una profesión con licencia de la nada; se necesita una infraestructura educativa completa. Por lo tanto, antes de que suceda, deberemos capacitar constantemente a los ingenieros de software en fiabilidad, seguridad, protección y otras responsabilidades. Necesitaremos un plan de estudios en colegios y universidades y formación continua para ingenieros, así como organizaciones profesionales que definan cómo será la acreditación, y las aumenten, y el tipo de recertificación que se necesita en este entorno tan cambiante. También necesitaremos descubrir cómo explicar la naturaleza internacional del desarrollo del software.

Nada de esto será fácil y es probable que se necesiten décadas para que funcione. La medicina tardó tres siglos en convertirse en una profesión en la Europa posterior al Renacimiento. Nosotros no podemos esperar tanto. Cualquier cosa que podamos hacer hoy para avanzar hacia una mayor profesionalidad beneficiará al campo en el largo plazo.

ACABAR CON LA FALTA DE COMPETENCIAS

Además de elevar los estándares profesionales, debemos aumentar drásticamente el número de personas dedicadas a la ciberseguridad.

La carencia de gente capacitada se denomina *falta de competencias en ciberseguridad* y ha sido un tema de conversación importante en casi todos los eventos de seguridad de TI a los que he asistido en los últimos años. No hay suficientes ingenieros de seguridad para satisfacer la demanda. Esto

ocurre en todos los niveles: administradores de red, programadores, arquitectos de seguridad, directivos y jefes de seguridad de la información.

Las cifras son aterradoras. Varios informes prevén que 1,5 millones, 2 millones, 3,5 millones o 6 millones de empleos de ciberseguridad quedarán sin cubrir en los próximos años debido a que la demanda está excediendo la oferta.[71] Cualquiera que sea la estimación correcta (y mi predicción se acerca más a la cifra más alta) podría suponer un desastre. Todas las soluciones de seguridad técnica discutidas en este libro requieren personas, y si no las tenemos, las soluciones no se implementarán.

Jon Oltsik, un analista de la industria que ha seguido de cerca este problema, dice lo siguiente: «La escasez de gente capacitada en ciberseguridad representa una amenaza existencial para nuestra seguridad nacional».[72] Dadas las tendencias actuales es difícil discutir tal afirmación.

La solución es obvia y difícil de implementar. Por el lado de la oferta, tenemos que exponer a los estudiantes a la ciberseguridad cuando sean niños, graduar a más ingenieros de software con una especialidad en ciberseguridad y crear programas de capacitación a mitad de carrera para cambiar a los ingenieros en ejercicio a la ciberseguridad. Necesitamos atraer a más mujeres y minorías a las carreras de ciberseguridad. Necesitamos invertir dinero en todo esto, y rápidamente.

Por el lado de la demanda, necesitamos automatizar esos trabajos siempre que sea posible. Ya estamos empezando a ver las ventajas de la automatización para la seguridad, y mejorará mucho una vez que empiecen a surtir efecto los beneficios del aprendizaje automático y la inteligencia artificial. Esto nos lleva directamente a mi siguiente recomendación.

AUMENTAR LA INVESTIGACIÓN

Tenemos serios problemas de seguridad técnica por resolver. Y, si bien ya hay mucha investigación y desarrollos en curso, necesitamos más investigación estratégica a largo plazo, de elevado riesgo y beneficios altos en tecnologías que pueda alterar drásticamente el equilibrio entre el atacante y el defensor. Hoy en día, hay muy pocos recursos dedicados a este tipo de I + D.

La mayoría de las organizaciones empresariales no se involucrarán en este tipo de investigación porque cualquier recompensa es lejana e indefinida. El grueso de las mejoras sustanciales en las próximas décadas será el resultado de investigaciones académicas financiadas por el Gobierno.

También necesitamos investigación aplicada a corto plazo y a pequeña escala. Las instituciones académicas no pueden hacerlo todo; las empresas también deben intervenir. Un crédito fiscal para la investigación podría proporcionar el incentivo adecuado para el desarrollo de productos y servicios seguros.

La investigación tiene el potencial de cambiar algunas de las suposiciones fundamentales sobre la seguridad de Internet+ discutidas en el capítulo 1. He visto propuestas para crear un Proyecto Manhattan cibernético,[73] una ciberllegada a la luna[74] y otras frases de moda similares. Sin embargo, no sé si estamos listos para algo así. Ese tipo de proyectos necesitan objetivos tangibles específicos. Un objetivo genérico, como mejorar la ciberseguridad, no lo logra.

Sea cual sea el mecanismo, necesitamos un proyecto de investigación y desarrollo conjunto y constante para las nuevas tecnologías que pueda protegernos contra la gran variedad de amenazas a las que nos enfrentamos ahora y a las que nos enfrentaremos en los próximos años y décadas. Es ambicioso, sí, pero no creo que tengamos ninguna alternativa. Lo que nos frena es la grave falta de confianza en el Gobierno por parte de la industria tecnológica.

Sin embargo esto no es nuevo. Esta llamada ya se ha hecho para el cambio climático, la alimentación y la superpoblación, la exploración espacial y muchos otros problemas a los que nos enfrentamos colectivamente.

CONSERVACIÓN Y MANTENIMIENTO DE FONDOS

Se habla mucho en Estados Unidos acerca de nuestra infraestructura nacional defectuosa (caminos, puentes, red hidráulica, escuelas y otros edificios públicos) y la necesidad de una inversión enorme para modernizarla. También deberíamos estar hablando de una gran inversión en nuestra infraestructura de Internet. No es tan antigua como nuestra infraestructura física, pero en algunos aspectos está igual de anticuada.

Los ordenadores se degradan más rápido que la infraestructura física convencional. Sabes que esto es cierto: es mucho más probable que actualices tu ordenador portátil y teléfono porque los modelos más antiguos no funcionan tan bien que tu coche o tu frigorífico. Compañías como Microsoft y Apple solo mantienen las versiones más recientes de sus sistemas operativos. Después de una década, en realidad, puede ser arriesgado seguir usando el hardware y el software de los ordenadores antiguos.

No vamos a reemplazar Internet con otra cosa; las tecnologías actuales están demasiado omnipresentes como para que eso funcione. Pero sí supondrá la actualización de piezas, de una en una, mientras se mantiene la compatibilidad con versiones anteriores. Necesitamos a alguien que coordine esta operación. También necesitamos que alguien financie el desarrollo y el mantenimiento de las piezas críticas de la infraestructura de Internet. Alguien debe trabajar con compañías de tecnología para ayudar a proteger las partes compartidas de la infraestructura y responder con rapidez a las vulnerabilidades cuando aparezcan. En el siguiente capítulo sostengo que el Gobierno es ese alguien.

Una vez que hayamos terminado de actualizar nuestra infraestructura de Internet crítica, tendremos que seguir actualizándola. La era en la que podías construir un sistema y hacer que funcionara durante décadas ha terminado (si alguna vez existió); los sistemas informáticos deben actualizarse continuamente. Necesitamos aceptar esta nueva y minimalista vida útil, tenemos que descubrir cómo mantener nuestros sistemas actualizados y tenemos que estar listos para pagar por ello. Y va a ser caro.

08

EL GOBIERNO ES EL QUE HABILITA LA SEGURIDAD

LOS AVIONES DEBERÍAN SER MUY PELIGROSOS. Estás dentro de lo que es básicamente un cohete volando por el aire a casi mil kilómetros por hora. Un avión moderno tiene más de seis millones de partes, muchas de las cuales tienen que funcionar a la perfección.[1] Si algo falla, el avión se estrella. El sentido común nos dice que es algo muy arriesgado.

Las aerolíneas compiten entre ellas en todo tipo de atributos: en precio y en rutas, en la inclinación de los asientos y en el espacio para las piernas, en los servicios que prestan en sus cabinas prémium, compiten en las difusas emociones de sentirse bien con una marca evocadora. Pero no compiten por la seguridad: la establece el Gobierno. Las compañías aéreas y los fabricantes de aviones deben cumplir con todo tipo de regulaciones, y todo esto es invisible para el consumidor, nadie promociona sus registros de seguridad en los anuncios. Aunque cada vez que subo a un avión (182 veces en 2017)[2] sé que el vuelo será seguro.

No siempre ha sido así. Los aviones eran muy peligrosos y los accidentes fatales bastante comunes. Lo que cambió fue la regulación de la seguridad.[3] A lo largo de décadas, el Gobierno ha impuesto mejora tras mejora en el diseño de los aviones, en los procedimientos de vuelo, en el entrenamiento de pilotos, etc. El resultado es que hoy en día los aviones comerciales son la forma más segura de viajar.[4]

Necesitamos hacer lo mismo con la seguridad de Internet. Hay varios modelos que considerar para establecer y hacer cumplir las normas de seguridad descritas en el capítulo 6. Una agencia examinadora independiente podría juzgar a los fabricantes por el cumplimiento de las normas. La Unión de Consumidores, una compañía sin ánimo de lucro financiada por suscripciones a revistas y subvenciones, podría ser un modelo. Podríamos confiar en el mercado, es decir, en que los clientes exigieran más seguridad al favorecer productos y servicios más seguros.

No soy optimista respecto a ninguna de estas ideas por todas las razones discutidas en el capítulo anterior. El Gobierno es, con diferencia, la manera más común de mejorar nuestra seguridad colectiva, y casi seguro que la más eficiente. Así es como cambiamos los incentivos comerciales. Así es como pagamos la defensa común. Así es como resolvemos problemas de acción colectiva y evitamos el gorroneo.

No puedo pensar en ninguna industria que en los últimos cien años haya mejorado su seguridad sin que la haya obligado a hacerlo el Gobierno. Esto ocurre con los edificios y los medicamentos, con la comida y los lugares de trabajo, con los automóviles, los aviones, las plantas de energía nuclear, los productos de consumo, los restaurantes y, más recientemente en Estados Unidos, los mecanismos financieros. En cada uno de esos casos, antes de la regulación gubernamental, los vendedores seguían produciendo productos peligrosos o dañinos y vendiéndoselos a un mercado ingenuo. Incluso cuando se manifestó una indignación popular fue necesario que el Gobierno cambiara el comportamiento de los dueños de los negocios. Desde el punto de vista de los fabricantes, es algo racional esperar lo mejor, en lugar de gastar dinero por adelantado para hacer que sus productos sean más seguros. Después de todo, es frecuente que los compradores no noten la diferencia hasta que algo sale mal, y los productores están predispuestos a preferir un beneficio inmediato (ahorro de costes) en lugar de un beneficio de seguridad a largo plazo.

Cuando los grupos industriales escriben sobre esto enfatizan que cualquier norma debe ser voluntaria.[5] Pero aquí es su interés personal el que habla. Si queremos que se cumpla un estándar, debe ser obligatorio. Cualquier otra cosa no va a funcionar, porque los incentivos no están alineados de forma correcta.

UN NUEVO ORGANISMO GUBERNAMENTAL

Los Gobiernos operan por núcleos. En el caso de Estados Unidos, la Administración de Drogas y Alimentos tiene jurisdicción sobre los dispositivos médicos; el Departamento de Transporte, sobre los vehículos terrestres; la Administración Federal de Aviación, sobre las aeronaves, aunque no considera las implicaciones de privacidad de los drones como parte de su mandato;[6] la Comisión Federal de Comercio supervisa la privacidad hasta cierto punto, pero solo en el caso de prácticas comerciales desleales o engañosas, y el Departamento de Justicia se involucra solo si se comete un delito federal.

En lo referente a los datos, la jurisdicción puede cambiar dependiendo de su uso. Si los datos se utilizan para influir en un consumidor, la Comisión Federal de Comercio (FTC, por sus siglas en inglés) tiene jurisdicción. Si esos datos se emplean para influir en un votante, es la jurisdicción de la Comisión Federal de Elecciones. Si, de la misma manera, esos mismos datos se usan para influir en un estudiante en una escuela, el Departamento de Educación es el pertinente. En Estados Unidos no existe ninguna autoridad cuyo ámbito de control sean los daños debidos a revelación de información o violaciones a la privacidad, a menos que la empresa involucrada haya hecho promesas falsas al consumidor. Cada organismo tiene su propio enfoque y sus propias reglas. Los comités del Congreso pelean por la jurisdicción, los departamentos y comisiones federales tienen sus propios dominios separados: desde la agricultura hasta la defensa, el transporte y la energía. A veces, los estados tienen organismos reguladores paralelos; por ejemplo, California ha sido líder durante mucho tiempo en temas de privacidad de Internet, y algunas veces el Gobierno federal se ha anticipado a las acciones estatales.

Así no es como va Internet. Internet, y ahora Internet+, es un sistema integrado de ordenadores, algoritmos y redes que funciona de una manera un poco anárquica. Es lo opuesto a un núcleo. Crece horizontalmente destruyendo las barreras tradicionales para que las personas y los sistemas que nunca antes se comunicaban puedan hacerlo. Ya sean grandes bases de datos personales, toma de decisiones algorítmicas, el Internet de las cosas, el almacenamiento en la nube o la robótica, son tecnologías que se interrelacionan entre sí de maneras muy profundas. Ahora mismo en mi teléfono inteligente existen aplicaciones que registran mi información de salud, controlan mi uso de energía e interactúan con mi vehículo. Este teléfono ha entrado en la jurisdicción de cuatro organismos federales diferentes de Estados Unidos: la FDA, el Departamento de Energía de Estados Unidos (DOE, por sus siglas en inglés), el Departamento de Transporte (DOT) y la Comisión Federal de Comunicaciones (FCC), y apenas ha comenzado.

Estas plataformas electrónicas son generales y necesitan un enfoque holístico de la política. Todos usan ordenadores y cualquier solución que se nos ocurra tendrá que ser global. No estoy diciendo que haya un conjunto de regulaciones que protejan todos los ordenadores en cada aplicación, pero tiene que haber un marco único aplicable a todas las computadoras, ya estén en un automóvil, un avión, un teléfono, un termostato o un marcapasos.

Estoy proponiendo un nuevo organismo federal: una oficina cibernética nacional. El modelo en el que me baso es la Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés), creada por el Congreso a raíz de los ataques terroristas del 11 de septiembre como una entidad única que coordina la inteligencia para todo el Gobierno de Estados Unidos. Su trabajo es establecer prioridades, coordinar actividades, asignar fondos y cruzar ideas. No es un modelo perfecto y se ha criticado a la ODNI por su ineficacia a la hora de coordinar los diferentes organismos. Pero suena al modelo que necesitamos para Internet+.

El propósito inicial de este nuevo organismo no sería regular, sino asesorar a otras áreas del Gobierno sobre temas que afectan a Internet+. Tales consejos serían muy necesarios para otros organismos federales y para los legisladores en todos los niveles gubernamentales. También podría dirigir la investigación cuando sea necesario, convocar reuniones entre las partes interesadas sobre diferentes temas y presentar informes de *amicus curiae* en casos judiciales en los que se valoraría su experiencia. En lugar de un organismo de aplicación, como la FTC o la FDA, tienes que verlo como la Oficina de Administración y Presupuesto o el Departamento de Comercio: un depósito de experiencia.

La institución que propongo reconocería que la política de Internet+ tendría que abarcar varios organismos más, que deberían conservar sus ámbitos de responsabilidad existentes. Pero muchas soluciones deben coordinarse de manera centralizada y alguien debe responsabilizar a los organismos individuales. Tanto el hardware como el software, los protocolos y sistemas de Internet+ se superponen entre aplicaciones muy diferentes.

Este nuevo organismo también podría gestionar otras iniciativas de seguridad en el Gobierno, así como actualizar el Marco de Ciberseguridad del NIST y desarrollar los otros tipos de estándares de seguridad que aparecen en el capítulo 6, al igual que la concesión de becas académicas y el crédito fiscal para investigación que mencionaba en el capítulo 7, requisitos que deberían formar parte del propio proceso de adquisición del Gobierno y de sus mejores prácticas. Podría gestionar las alianzas entre el Gobierno y la industria y ayudar a desarrollar estrategias que incluyan a ambos. También serviría como un contrapeso para las organizaciones gubernamentales militares y de seguridad nacional que ya están estableciendo políticas en este espacio. Hoy en día, están haciendo algo en este sentido el Instituto Nacional de Estándares y Tecnología y la Fundación Nacional para la Ciencia (NSC, por sus siglas en inglés), pero ni uno ni otro podrían modificarse con facilidad para este nuevo

rol, por lo que tendría sentido trasladar estas funciones al nuevo organismo dedicado a estos menesteres.

Y, por último, este organismo sería un lugar para que el Gobierno consolidara su experiencia. Un organismo dedicado a Internet+ podría atraer (y pagar salarios competitivos) a personas con talento que ayudaran a elaborar y asesorar en asuntos de políticas. Esto significa que estaría formado por ingenieros e informáticos trabajando en estrecha colaboración con expertos en derecho y en políticas. Este es un tema al que volveré en la conclusión: la importancia de que los tecnólogos y los responsables de la formulación de políticas mantengan una colaboración estrecha.

Una vez establecido el organismo, podrían crearse otros centros de excelencia que trabajaran bajo su paraguas. De nuevo, el ODNI es un buen modelo, con su Centro Nacional de Contraterrorismo y el Centro Nacional de Contraproliferación. Imagino que el nuevo organismo podría necesitar un centro nacional de inteligencia artificial y un centro nacional de robótica, y tal vez incluso un centro nacional de algoritmos. Podríamos crear una academia nacional de ciberdefensa, una instalación interinstitucional con una variedad de clases, certificaciones y registros adonde todos los organismos podrían enviar personal para su capacitación. También tendría que coordinarse estrechamente con el Departamento de Seguridad Nacional y probablemente con el Departamento de Justicia.

Al final, de alguna manera la regulación tendrá que abarcar varios dominios de Internet+. Tal vez este nuevo organismo sea el regulador, pero es más probable que los ya existentes, que ya regulan varias industrias, continúen haciéndolo y agregando las regulaciones de seguridad de Internet+ a sus portafolios. Sus amplios mandatos los hacen más ágiles que el Congreso. Pueden responder a los cambios en tecnología o en los mercados y pueden motivar a las empresas a cambiar sus comportamientos.

Un modelo basado en la FTC podría ser útil. La FTC no tiene reglas específicas; en cambio, tiene reglas vagas y resultados previstos, y persigue a los infractores más flagrantes. Todos los demás observan las acciones y multas de la FTC e intentan ser un poco mejores que las empresas que reciben sanciones. La FTC también orienta y trabaja con la industria para promover su cumplimiento. Y aunque a veces se describe como falta de poder, sus resultados son el conocimiento público de las normas de conducta comercial aceptable, la asunción de responsabilidades para aquellos que las violaron y la mejora continua en todos los ámbitos.

Aquí hay un ejemplo: en 2006, Netflix publicó cien millones de reseñas y calificaciones anónimas de películas como parte de un concurso.[7] Los investigadores pudieron desanonimizar algunos de esos datos,[8] lo que sorprendió a casi todo el mundo.[9] La FTC solo tomó medidas contra Netflix cuando vio que la compañía no había aumentado su preocupación por los datos de los clientes al año siguiente, cuando volvió a realizar el concurso.[10]

Hoy en día, tanto la Comisión Federal de Comunicaciones como la Comisión de Bolsa y Valores estadounidenses tienen autoridad para exigir a las empresas que cotizan en bolsa que auditen y luego certifiquen su propia ciberseguridad.[11] Esos organismos podrían tomar un marco de seguridad existente y usarlo, o crear uno propio.

No soy el primero que sugiere esto. Un grupo de investigación que asesoraba a la Comisión Europea propuso la formación de la Agencia Europea de Ingeniería de Seguridad y Protección;[12] Ashkan Soltani, antiguo tecnólogo jefe de la Comisión Federal de Comercio, propuso una nueva Comisión Federal de Tecnología;[13] Ryan Calo, profesor de Derecho en la Universidad de Washington, ha propuesto una Comisión Federal de Robótica, [14] y Matthew Scherer, de la Universidad George Mason, ha propuesto un organismo para regular la inteligencia artificial.[15]

Algunos otros países están considerando esta misma línea de actuación. Israel creó la Oficina Cibernética Nacional en 2011 para reforzar la defensa del país en el ciberespacio y asesorar al resto del Gobierno sobre temas relacionados con la cibernética.[16] Reino Unido creó el Centro Nacional de Seguridad Cibernética en 2016 con el siguiente fin: «Ayudar a proteger nuestros servicios críticos de ataques cibernéticos, gestionar incidentes graves y mejorar la seguridad subyacente de Internet del Reino Unido a través de mejoras tecnológicas y asesoramiento a ciudadanos y organizaciones».[17] En mi opinión, ambas organizaciones están demasiado vinculadas al ejército y, por lo tanto, a la parte del Gobierno que depende de la inseguridad de Internet, pero son un comienzo.

Hay un precedente histórico significativo en Estados Unidos para esta idea. Las nuevas tecnologías suelen conducir a la creación de nuevos organismos gubernamentales. Los trenes lo hicieron, igual que los automóviles o los aviones. La invención de la radio llevó a la formación de la Comisión Federal de Radio, que se convirtió en la Comisión Federal de Comunicaciones. La invención de la energía nuclear llevó a la formación de la Comisión de Energía Atómica, que se convirtió en el Departamento de Energía.

Podemos debatir los detalles y los límites apropiados de este nuevo organismo y su estructura organizativa. Pero, sea cual sea el formato, necesitamos un organismo gubernamental que esté a cargo de esto.

Creo que la regulación de la era de Internet será diferente de la regulación de la era industrial. Internet ya se rige por un modelo con múltiples partes interesadas, en el que los Gobiernos, la industria, los tecnólogos y la sociedad civil se unen para resolver los problemas relacionados con el funcionamiento de Internet. Supongo que este modelo es mucho más adecuado para la regulación de Internet+ que el resto de los modelos a los que estamos acostumbrados.

Hay objeciones razonables a esta propuesta. Los organismos gubernamentales son ineficientes. A menudo carecen de la experiencia necesaria. Son burocracias y carecen de visión y previsión. Existen problemas en la velocidad, el alcance, la eficacia y en el potencial de captación reguladora. Y, por supuesto, existe la opinión generalizada de que el Gobierno tan solo debería apartarse.

Pero esas preocupaciones existen independientemente de si hay un único organismo gubernamental nuevo o si la autoridad se repartiría entre una docena o más de organismos ya existentes. El valor de un solo organismo es considerable. La alternativa es crear una política de Internet+ *ad hoc* y por partes de una manera que agregue complejidad y no contrarreste las amenazas emergentes.

Por supuesto, el problema son los detalles. Mi idea de esta nueva oficina cibernética podría no funcionar, y estoy de acuerdo con eso. Espero, como mínimo, iniciar un debate.

REGULACIONES GUBERNAMENTALES

La industria informática ha estado en gran medida libre de regulaciones. Esto se debe en parte a que se trata de una industria emergente y en parte a su relativa inocuidad inicial y a la falta de voluntad de sus líderes de reconocer cuánto han cambiado las cosas. Y es sobre todo el resultado de la reticencia gubernamental a arriesgarse a detener el enorme generador de riqueza en que se ha convertido Internet. Creo que estos días están llegando a su fin y que la regulación de Internet+ es inevitable. Hay varias razones.

Una, los Gobiernos tienden a regular las industrias que son cuellos de botella para la economía en general, como las telecomunicaciones y el transporte.[18] Internet+ es sin duda una de ellas, y es cada vez más una pieza

clave en la economía. Dos, los Gobiernos regulan los productos y servicios de consumo que pueden matar a las personas, e Internet+ se está uniendo deprisa al club. Tres, muchas industrias ya existentes en las que están presentes un gran número de ordenadores, desde los juguetes hasta los electrodomésticos, los automóviles y las plantas de energía nuclear, ya están reguladas.

Es importante darse cuenta de que la regulación es más que una lista de cosas obligatorias o prohibidas. Esa es la forma más contundente de regulación, pero la mayoría de las veces está más matizada. La regulación puede crear responsabilidades y dejar los detalles para el mercado, empujar en una u otra dirección, cambiar los incentivos, empujar en lugar de forzar o puede ser lo bastante flexible como para adaptarse a los cambios en las expectativas de la tecnología y de la sociedad.

El objetivo no es ser perfeccionista. No exigimos que los fabricantes de automóviles produzcan el coche más seguro posible, sino establecer normas de seguridad como el uso de cinturones y airbags o realizar pruebas de colisión, y le dejamos el resto al mercado. Este enfoque es esencial en un entorno tan dinámico como el de Internet+.

Europa ya está incrementando considerablemente sus regulaciones de Internet (hablaremos sobre el Reglamento General de Protección de Datos de la UE en el capítulo 10) y algunos estados de Estados Unidos se están moviendo en una dirección similar. Si bien en Washington hay poca apetencia de cualquier tipo de regulación, podría aumentar con rapidez si ocurre un desastre que se cobre un gran número de vidas o destruya una cierta parte de nuestra economía.

Estados Unidos ha comenzado a regular cosas a nivel federal, pero apenas empieza a adaptarse y solo en una parte específica de la industria. Por ejemplo, la FDA emitió una guía para los fabricantes de dispositivos médicos sobre los requisitos reglamentarios para aquellos conectados a Internet. Este organismo no realiza las pruebas por sí mismo, sino que son los desarrolladores quienes prueban sus productos y servicios según los estándares y le envían su documentación a la FDA para que esta los apruebe.[19] Es un asunto serio. La FDA no titubea a la hora de negar la aprobación de productos que fallan o de exigir la retirada de los que causan daños.

Las reglas para la privacidad de los datos médicos de los pacientes son sustancialmente diferentes de las que rigen la privacidad de los datos del consumidor.[20] Como debería esperarse, las reglas de los datos médicos son mucho más estrictas. Muchos desarrolladores de productos nuevos y de servicios relacionados con la salud están tratando de posicionar sus productos

como dispositivos de consumo, por lo que no requieren la aprobación de la FDA. Esto a veces funciona, como sucede con las pulseras de actividad tipo Fitbit. Y a veces la FDA responde, como lo hizo con los datos genéticos recopilados por 23andMe.[21]

Para automóviles, el Departamento de Transporte solo ha emitido estándares de seguridad voluntarios; aunque nunca son tan efectivos como los obligatorios, pueden ayudar. Por ejemplo, en una demanda, el tribunal a menudo evaluará el cumplimiento voluntario de la guía del departamento para ayudar a determinar si un fabricante fue negligente.

La Administración Federal de Aviación (FAA, por sus siglas en inglés) ha adoptado un enfoque diferente con la regulación de los drones. La FAA no requiere certificación de diseño para cada nuevo dron que sale al mercado; en cambio, regula de forma indirecta los drones de consumo mediante políticas que restringen cómo y dónde pueden usarse.

Ha habido algunas victorias. En 2015, la FTC demandó a los hoteles Wyndham por la seguridad de sus ordenadores.[22] La empresa tenía prácticas de seguridad terribles que permitían que los piratas informáticos entraran repetidamente en sus redes y robaran datos de sus clientes. La FTC argumentó que Wyndham tenía una política de privacidad que hacía promesas que la compañía no cumplía, por lo que estaba engañando a sus clientes.

La batalla judicial fue complicada, pues en gran parte dependía de asuntos de autoridad que no son relevantes aquí. Pero lo que resulta interesante es que una de las líneas de defensa de Wyndham fue que la FTC no podía multarlos por no ser lo bastante seguros, pues la FTC nunca le había dicho a la cadena hotelera qué significaba *bastante seguro* en primer lugar. El Tribunal Federal de Apelaciones se puso del lado de la FTC y básicamente dijo que la tarea de Wyndham era averiguar qué significaba ser lo bastante seguro y que había fracasado al no intentar hacerlo.[23]

DESAFÍOS DE LA REGULACIÓN

Internet es el entorno más dinámico que existe. La regulación, en especial la errónea o excesiva, puede retrasar las nuevas tecnologías y las innovaciones. En seguridad puede inhibir la flexibilidad y la agilidad necesarias para mantenerse al día con las amenazas cambiantes.

Cuando hablamos de regular Internet+, observo cuatro problemas: la velocidad, el alcance, la eficacia y el potencial de asfixiar a las industrias regulándolas.

Primero, la velocidad: el cambio de las políticas gubernamentales es lento en comparación con la velocidad de la innovación tecnológica, aunque solía ser al revés. Pasaron casi cuarenta años desde que Alexander Graham Bell comercializara por primera vez el teléfono hasta que se convirtió en un elemento cotidiano. Con la televisión se tardó más de treinta años. Esos días han terminado. Los correos electrónicos, los teléfonos móviles, Facebook o Twitter penetraron en la sociedad mucho más rápido que las tecnologías de las décadas anteriores. (Facebook tardó trece años en acumular 2.000 millones de usuarios regulares en todo el mundo.)[24] Estamos en un punto en el que la ley siempre se quedará atrás con respecto a la tecnología: para cuando se emiten los reglamentos, a menudo ya están desfasados. Un buen ejemplo son las regulaciones de la UE que requieren avisos sobre las *cookies* en los sitios web; esto hubiera tenido sentido en 1995, pero, cuando el reglamento entró en vigor en 2011, el seguimiento web era mucho más complejo. De igual forma, los tribunales siempre intentarán aplicar leyes anticuadas a situaciones más modernas y, lo que es peor, los cambios tecnológicos darán lugar a que las leyes tengan todo tipo de consecuencias no deseadas.

A continuación, el alcance: las leyes tienden a redactarse de forma restringida, centradas en tecnologías específicas. Estas leyes pueden fallar cuando las tecnologías cambian. La mayoría de nuestras leyes de privacidad se redactaron en la década de los setenta, y si bien las preocupaciones no han cambiado, la tecnología sí lo ha hecho. Aquí hay un ejemplo: la Ley de Privacidad de Comunicaciones Electrónicas estadounidense se aprobó en 1986. Una de las cosas que hizo fue regular la privacidad de los correos electrónicos al proporcionar diferentes protecciones de privacidad para dos tipos de correo electrónico: para acceder al correo recibido recientemente el Gobierno necesita una orden judicial; para acceder al correo que ha permanecido en el servidor durante más de 180 días, el Gobierno puede realizar búsquedas sin restricciones. En 1986 esto tenía sentido, ya que el almacenamiento era caro. Las personas hacían que su proveedor de correo electrónico llevara el correo desde el servidor hasta su ordenador. Cualquier cosa dejada en el servidor durante más de seis meses se consideraba abandonada, y no tenemos derechos de privacidad sobre la propiedad abandonada. Hoy todo el mundo deja su correo electrónico en el servidor durante seis meses o incluso seis años. Así es como funcionan Gmail, Hotmail y cualquier otro proveedor de correo electrónico basado en la Red. La ley hace una distinción importante entre los servicios que proporcionan

comunicación y los que procesan y almacenan datos, una distinción que ya no tiene sentido.[25] La lógica detrás de esa antigua ley ha sido revertida por completo por la tecnología, y sin embargo sigue vigente.[26]

Esto sucederá de forma reiterada hasta que comencemos a redactar leyes que sean más generales de modo que incluyan no solo los sistemas actuales sino también los que puedan surgir en un futuro. Si nos centramos en los aspectos humanos de la ley, en lugar de en los aspectos tecnológicos, podremos proteger las leyes contra los problemas de velocidad y de alcance. Por ejemplo, podríamos redactar leyes que abordaran la comunicación, independientemente de si se trata de voz, vídeo, correos electrónicos, mensajes de texto, mensajes privados o cualquier tecnología que aparezca más adelante. Nuestro futuro tecnológico está lleno de propiedades emergentes de las nuevas tecnologías, y nos sorprenderemos con frecuencia.

Hay otro problema de alcance con las regulaciones, y es por completo diferente. ¿Cómo de generales debemos hacerlas? Por un lado, es obvio que necesitamos unos estándares diferentes para automóviles y aviones que los que tenemos para juguetes y otros objetos domésticos, así como diferentes regulaciones para las bases de datos financieras y el tráfico anónimo de datos. Por otro lado, la interconexión de todo hace que los juguetes y los agujeros de datos parezcan más inocuos de lo que son.

Además, es difícil saber dónde deberían detenerse exactamente las regulaciones. Sí, vamos a regular las cosas que afectan al mundo de una manera física directa, pero como todo está interconectado y las amenazas también, es imposible separar cualquier parte de Internet+ y decir que no importa. Alguien podría sugerir que no es necesario molestarse en regular los dispositivos de Internet de bajo coste, pero las vulnerabilidades en estos podrían afectar la infraestructura crítica. Otros podrían sugerir la exención de los sistemas de software puro porque no son físicos, pero estos pueden tener efectos reales: Piensa en un software que decida a quién se le concede la libertad bajo fianza o a quién la libertad condicional. Las regulaciones probablemente también deberían cubrir estos sistemas.

El tercer problema con la regulación de Internet+ es la eficacia. Las grandes empresas son muy efectivas evadiendo normas. Las compañías tecnológicas más importantes están gastando cantidades récord de dinero para presionar políticamente en Washington, hasta el punto de que ahora invierten el doble que la industria bancaria y muchas veces más que las compañías petroleras, los contratistas de defensa y todos los demás.[27] Solo Google gastó seis millones de dólares en persuasión política durante tres meses en

2017.[28] E incluso sin grupos de presión, se trata de empresas generadoras de enormes riquezas para Estados Unidos, y el Congreso no está dispuesto a arriesgarse a acabar con ello.

Ya estamos viendo algunos ejemplos. Uno es la forma en que los desarrolladores de pulseras de actividad trabajaron para convencer a la FDA de que sus productos no eran dispositivos médicos y, por lo tanto, no debían estar sujetos a sus normas.[29] Los intermediarios de datos han realizado maniobras de presión similares con respecto a la información personal en sus bases de datos.[30] Como dijo la profesora de leyes de privacidad Julie Cohen: «el poder interpreta la regulación como daño y se mueve a su alrededor».[31]

Necesitamos regular de manera justa y hacerlo bien. Ambas cosas son difíciles en la práctica. Muchas regulaciones no funcionan. Ya hemos visto ejemplos de esto en la seguridad de Internet: la ley CAN-SPAM (Ley de Control y Asalto a la Pornografía y Marketing No Solicitado) que no detuvo el spam,[32] la Ley de Protección de la Privacidad Infantil en Línea, que no protege a los niños, y la ley DMCA, que no impidió la realización de copias no autorizadas. Veremos más propuestas legislativas ineficaces y contraproducentes en el capítulo 11.

Y la regulación es tan efectiva como su ejecución. En Estados Unidos, la FTC ha emprendido acciones legales contra las llamadas automáticas,[33] los infractores de llamadas a los números inscritos en el Registro Nacional de No Llamar,[34] los anunciantes de llamadas engañosas[35] y la recogida excesiva de datos por parte de juguetes[36] y televisores.[37] Las multas de la FTC van desde unos pocos cientos de miles de dólares hasta millones. Pero el organismo no es muy eficiente al disponer de unos recursos limitados para investigar y presentar casos, lo que les permite a las empresas más inteligentes evadir las regulaciones de la FTC quizá de forma indefinida. Las posibilidades de que te atrapen y te demanden con éxito son tan bajas que cualquier compañía sensata asumiría el riesgo.

Las regulaciones son constantemente manipuladas. En lugar de promover el bien común, su objetivo es fomentar una agenda privada. Esto sucede siempre, pero el ejemplo más cercano a mi campo de acción es la oficina de derechos de autor: no se trata de la voz de la gente y sus regulaciones no están diseñadas para promover la justicia, sino que es la voz de los titulares de los derechos de autor, de las grandes empresas como Disney, y sus reglamentos están diseñados en gran medida para promover los intereses de esas empresas. Podría decir lo mismo acerca de muchas industrias y de los organismos que se supone que deben regularlas. Es una captación reguladora, y podría gastar un

capítulo entero en ello. Es algo muy común y ocurre por muchas razones, por lo que no veo ningún motivo por el que la regulación de Internet sea inmune a las mismas fuerzas. Si los reguladores se convierten en el brazo ejecutor de un grupo industrial afianzado, los resultados pueden ser peores que no hacer nada en absoluto.

El cuarto y último problema con las regulaciones es que pueden frenar la innovación. Creo que solo tenemos que aceptarlo y, en algunos casos raros, querremos hacerlo deliberadamente. La innovación sin restricciones solo es aceptable para tecnologías inocuas. A menudo, ponemos límites a las tecnologías que pueden matarnos porque creemos que la seguridad vale la pena. El principio de precaución indica que, cuando el potencial de daño es grande, nos equivocamos al implementar una nueva tecnología sin pruebas de seguridad. Esta manera de pensar será más importante en un mundo en el que un atacante pueda abrir todas las cerraduras de las puertas o piratear todas las centrales eléctricas.[38] No queremos y no podemos detener el progreso tecnológico, pero podemos tomar decisiones meditadas entre futuros tecnológicos o acelerar o retrasar ciertas tecnologías con respecto a las demás.[39]

No obtendremos nuevas funciones para nuestros ordenadores y dispositivos al mismo ritmo que estamos acostumbrados, y eso será un beneficio cuando esas características pueden matarte. Pero, como he mencionado un par de veces, las regulaciones también pueden fomentar la innovación. Al proporcionar incentivos a la industria privada para resolver problemas de seguridad, es probable que obtengamos más seguridad.

Tendremos que trabajar con cuidado en todo esto. Algunas regulaciones podrían sobrecargar de manera desproporcionada a las pequeñas empresas en las que tiene lugar la innovación tecnológica. A menudo benefician a quienes tienen el dinero y acaban funcionando como una barrera de entrada para los nuevos competidores en lugar de fomentar la competencia. No quiero minimizar el asunto, aunque hemos lidiado con este tipo de problemas en otras industrias, y confío en que también podamos encontrar el término medio aquí.

NORMAS, TRATADOS Y ORGANISMOS REGULADORES INTERNACIONALES

Bueno, lo admito: he hecho trampa durante todo este capítulo al ignorar la naturaleza internacional del problema. ¿Cómo puedo proponer que los

ciudadanos de Estados Unidos promulguen regulaciones nacionales para resolver lo que es inherentemente un problema internacional? Incluso aunque Estados Unidos y la UE aprueben estrictas regulaciones sobre la seguridad del IoT, ¿qué impide que los productos baratos inseguros lleguen a las fronteras de Asia o de otro lugar?

Es una crítica justa. Los países pueden regular lo que se fabrica o vende dentro de sus fronteras; muchos ya lo hacen para casi todos los productos de consumo. Podemos crear una lista negra de productos o de fabricantes, y obligar a compañías como Amazon y Apple a eliminarlos de sus tiendas en línea, pero eso solo funcionará hasta cierto punto. A menos que dejemos que nos sometan a búsquedas generalizadas e invasivas, no podemos regular lo que cruza las fronteras en maletas, paquetes de pedidos por correo o descargas de Internet. No podemos regular los servicios de software comprados en sitios web extranjeros; censurarlos no es una opción. Esto no es nada nuevo y es algo con lo que tendremos que lidiar.

Aun así, las regulaciones nacionales pueden tener un efecto poderoso en todo el mundo. Al contrario que los fabricantes de automóviles, que venden productos diferentes en cada país según las leyes de control de emisiones, el software es más bien un tipo de negocio que se vende en cualquier lugar una vez que se escribe. Si un mercado lo bastante grande regula un producto o un servicio de software, es presumible que el fabricante realice ese cambio en todo el mundo en lugar de tener que mantener varios productos. Debido a que Internet es global, la regulación de la ciberseguridad es un poco como imponer estándares de emisiones: si un país lo hace por su cuenta, asume todos los costes, mientras que el resto del mundo comparte los beneficios.

La cooperación internacional está llegando.[40] En ocasiones, a los Gobiernos les interesa armonizar las leyes, la mayoría de los países están preocupados por proteger sus economías e infraestructuras de la interrupción, los Estados también consideran la cooperación para combatir el crimen cibernético y los grupos de delincuencia organizada inteligentes se involucran en lo que yo llamo *arbitraje jurisdiccional*: elegir países específicos con leyes de delitos cibernéticos laxas donde ubicar la actividad criminal, fuerzas policiales fácilmente sobornables y sin tratados de extradición. Sabemos que tanto Rusia como China hacen la vista gorda ante el crimen dirigido al exterior. Hay otros paraísos de hackers en Nigeria, Vietnam, Rumanía y Brasil.[41] Para los países pobres, el crimen cibernético organizado puede ser en realidad una fuente de riqueza y de prosperidad. Otros países, como Corea

del Norte, participan activamente en la ciberdelincuencia patrocinada por el Estado para llenar las arcas del régimen.[42]

Se han dado algunos avances prometedores en este sentido. Existen cientos de equipos nacionales de respuesta ante emergencias informáticas (verás que se llaman CERT o CSIRT, por sus siglas en inglés) en todo el mundo. Estos grupos cooperan con frecuencia más allá de las fronteras y es una manera de compartir información. La Convención de Budapest fue ratificada por 52 países, aunque no por algunos de los actores más importantes, como Rusia, Brasil, China e India. Este tratado proporciona un marco para la cooperación policial y judicial internacional en materia de delitos informáticos.[43]

No queremos que los Gobiernos gestionen Internet. Gran parte de la innovación de la Red se deriva de la inocua negligencia del Gobierno de Estados Unidos. Hoy en día, los países de todo el mundo quieren involucrarse mucho más en la gestión del Internet doméstico. En casos extremos, países grandes y poderosos, como Rusia y China, quieren controlar su Internet doméstico de manera que aumente la vigilancia, la censura y el control sobre sus ciudadanos.[44]

El modelo de gobierno actual para Internet es múltiple: se compone de Gobiernos, empresas, sociedad civil y tecnólogos interesados. Por disfuncional que pueda parecer a veces, es nuestra mejor defensa contra un Internet inseguro. También evita una división (llamada *balcanización*) de Internet que podría dar como resultado países totalitarios imponiendo sus propias demandas.

Las normas (reglas informales para individuos, corporaciones y naciones con un comportamiento aceptable) regulan mucho más en nuestra sociedad de lo que la mayoría de las personas son conscientes. Sin embargo, en la actualidad no tenemos normas internacionales establecidas para los usuarios de armas cibernéticas, y la norma vigente respecto al ciberespionaje dice que este es aceptable. Como ya vimos en el capítulo 4, los países están en medio de una carrera cibernética de armas y cada uno de ellos está inventándosela a medida que avanza.

El politólogo Joseph Nye cree que los países pueden desarrollar normas que limiten los ataques cibernéticos.[45] Por varias razones, argumenta que está en el propio interés de las naciones alcanzar acuerdos como no atacar las infraestructuras de las demás en tiempos de paz o no usar las armas cibernéticas contra civiles en tiempos de guerra. Estas normas al final encontrarán su camino hacia los tratados y otros acuerdos más formales.

Un obstáculo para el consenso es que muchos países no piensan en la ciberseguridad como la prevención de un ataque por parte de un agresor hostil, sino también como garantía de que opiniones contrarias no influyan en la política interna. El contenido viral disconforme puede representar una amenaza tan grande como el código viral. Esto hace que la negociación multilateral sea difícil, aunque no imposible.

Naciones Unidas tenía su Grupo de Expertos Gubernamentales sobre Desarrollo en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (GGE, por sus siglas en inglés), que presentó una buena lista de normas acordadas internacionalmente en 2013,[46] pero fueron bloqueadas de inmediato por países como China, que no estaba de acuerdo con ellas, y, en 2017, el grupo se disolvió tras llegar a un punto muerto.[47]

Aun así, es probable que haya algunos puntos en común. Si los Estados no pueden ponerse de acuerdo en no acumular armas cibernéticas, por ejemplo, es plausible, no obstante, que puedan aceptar algunos estándares de no proliferación para las armas cibernéticas. La Iniciativa de Seguridad contra la Proliferación (PSI, por sus siglas en inglés) ha tenido un éxito relativo en el tratamiento del tráfico ilegal de armas de destrucción masiva. Más de cien países, incluida la generalmente disconforme Rusia, han aceptado involucrarse. La idea es prevenir la proliferación de armas estableciendo mejores estándares de seguridad y controles de exportación, interceptando los materiales para armas de destrucción masiva y mediante el intercambio de información y ejercicios de desarrollo de capacidades.

Habrá problemas de cumplimiento con cualquier acuerdo. Las armas cibernéticas son fáciles de ocultar a los inspectores de tratados, y las capacidades ofensivas se parecen mucho a las defensivas.[48] Pero los primeros tratados nucleares firmados en la década de 1960 también tuvieron problemas y, sin embargo, comenzaron lo que, en retrospectiva, fue un proceso exitoso que convirtió al mundo en un lugar mucho más seguro.

Algunas ideas sobre cómo empezar el camino hacia un acuerdo internacional de ciberseguridad ya están sobre la mesa. En un informe de 2014, el experto en política cibernética Jason Healey recomendó crear un régimen regulador internacional similar al establecido tras la crisis financiera mundial de 2008.[49] En el mismo año, Matt Thomlinson, de Microsoft, propuso un grupo G20+20 de veinte Gobiernos y veinte compañías mundiales de tecnologías de la información y las comunicaciones para que redactaran un conjunto de principios para el comportamiento aceptable en el ciberespacio.

[50] El presidente y director jurídico de Microsoft Brad Smith propuso una *Convención de Ginebra* para el ciberespacio que estableciera qué parte de él está fuera del alcance de la interferencia gubernamental.[51] Y Google tiene su propia propuesta.[52] En este punto, las ideas son claramente muy ambiciosas.

Establecer normas es un proceso largo. Es probable que lleguemos más lejos con la cooperación gradual y los acuerdos que con el esfuerzo por lograr una gran negociación perfecta de inmediato. Y aun así habrá países que no cumplirán con ninguna regla, norma, guía o cualquier otra cosa que encontremos. Trataremos esto de la misma manera que lo hacemos en cualquier otra área de derecho internacional. No será perfecto, pero trabajaremos en ello y lo mejoraremos con el tiempo.

Por desgracia, en Estados Unidos estamos estableciendo normas con nuestro propio comportamiento. Al utilizar Internet tanto para la vigilancia como para el ataque, estamos diciéndole al mundo que eso están bien. Al dar prioridad a la ofensiva sobre la defensa, estamos haciendo que el mundo sea menos seguro.

09

CÓMO LOS GOBIERNOS PODRÍAN PRIORIZAR LA DEFENSA SOBRE EL ATAQUE

SI LOS GOBIERNOS VAN A REPRESENTAR el papel principal en la mejora de la seguridad de Internet+, como he estado afirmando que es su deber, necesitan cambiar sus prioridades. En este momento, priorizan el mantenimiento de la capacidad de usar Internet para fines ofensivos, como exponía en el capítulo 4. Pero, si alguna vez progresamos en materia de seguridad, los Gobiernos deberán cambiar su forma de pensar y comenzar a priorizar la defensa; deben apoyar lo que Jason Healey llama estrategia de *defensa dominante*.[1]

Sí, la ofensiva es esencial para la defensa. Las organizaciones de inteligencia y de aplicación de la ley en las democracias liberales tienen necesidades justificadas para controlar a los Gobiernos hostiles, vigilar a las organizaciones terroristas e investigar a los delincuentes. Utilizan la desprotección de Internet+ para hacer todas estas cosas y hacen reclamaciones legítimas sobre los beneficios de seguridad resultantes. No se caracterizan por ser antiseguridad; de hecho, su retórica está muy a favor de la seguridad, pero sus acciones la socavan.

La NSA tiene dos misiones: vigilar las comunicaciones de los Gobiernos de otros países y proteger las comunicaciones del Gobierno de Estados Unidos contra la vigilancia.[2] En el antiguo mundo de las redes punto a punto, estas misiones eran complementarias, porque los sistemas no se superponían. La NSA podía descubrir cómo vigilar un enlace de comunicaciones navales entre Moscú y Vladivostok y usar esa experiencia para proteger el enlace de comunicaciones navales entre Washington y Norfolk. Las escuchas ilegales en los sistemas de comunicaciones del Pacto Soviético y del Pacto de Varsovia no afectaron a las comunicaciones estadounidenses porque los sistemas de radio eran diferentes. Sabotear los ordenadores militares chinos no afectó a los estadounidenses porque los ordenadores eran diferentes. En un mundo donde los ordenadores eran raros,

las redes lo eran aún más y la interoperabilidad estaba hecha a medida, por lo que las acciones de la NSA en el extranjero no tenían efecto en el interior de Estados Unidos.

Esto ya no es así. Con pocas excepciones, todos usamos los mismos ordenadores y teléfonos, los mismos sistemas operativos y las mismas aplicaciones; todos usamos el mismo hardware y software de Internet. No hay forma de proteger las redes de Estados Unidos y dejar al mismo tiempo las redes extranjeras abiertas a escuchas y ataques. No hay manera de proteger nuestros teléfonos y ordenadores frente a criminales y terroristas sin que también protejamos sus propios teléfonos y ordenadores. En la red mundial generalizada que es Internet, cualquier cosa que hagamos para proteger el hardware y software tiene efecto en todo el mundo. Y todo lo que hacemos para mantenerlo inseguro afecta de igual manera al mundo entero.

Esto nos enfrenta a una elección: o bien protegemos nuestras cosas y como efecto secundario también las suyas, o bien mantenemos sus cosas vulnerables y como efecto secundario también las nuestras. En realidad, no es una elección difícil. Una analogía podría ser una casa. Imagina que todas las casas pudieran abrirse con una llave maestra y que esto lo supieran los criminales. Reparar las cerraduras también significaría que las casas seguras de los delincuentes estarían más protegidas, pero está bastante claro que proteger las casas de todos compensaría esa parte negativa. Con un Internet+ incrementando dramáticamente los riesgos de la inseguridad, la elección es aún más obvia. Debemos proteger los sistemas de información utilizados por nuestros funcionarios electos, nuestros proveedores de infraestructuras críticas y nuestros negocios.

Sí, aumentar nuestra seguridad nos hará más difícil escuchar a escondidas y atacar a nuestros enemigos en el ciberespacio. (No hará imposible que los agentes de la ley resuelvan los delitos; abordaré eso más adelante en este capítulo). En cualquier caso, vale la pena. Si alguna vez vamos a proteger Internet+, debemos priorizar la defensa por encima de la ofensiva en todos sus aspectos. Tenemos más que perder a través de nuestras vulnerabilidades de Internet+ que nuestros adversarios, y mucho más que ganar con la seguridad de Internet+. Tenemos que reconocer que los beneficios de seguridad de un Internet+ protegido superan con creces los beneficios de seguridad de uno vulnerable.

Esta es mi propuesta de lo que Estados Unidos y otros Gobiernos democráticos deberían hacer para anteponer la defensa al ataque. Llevar a cabo estas acciones contribuirá en gran medida a proteger Internet+. Aún más

importante, el cambio de prioridades de la ofensiva a la defensa permitirá a los Gobiernos cumplir con el papel tan necesario de los facilitadores de seguridad de Internet+.

DIVULGAR Y CORREGIR VULNERABILIDADES

Recordemos el capítulo 2, en el que hablaba sobre las vulnerabilidades del software. Estas tienen usos tanto ofensivos como defensivos, y, cuando alguien descubre una, hay que tomar una decisión: elegir la defensa significa alertar al vendedor y repararla; elegir la ofensa significa mantener la vulnerabilidad en secreto y usarla para atacar a otros.

Si una unidad cibernética militar ofensiva, o un fabricante de armas cibernéticas, descubre una vulnerabilidad, la mantiene en secreto para poder explotarla. Si se usa con cautela, puede permanecer oculta durante mucho tiempo; si no se usa, seguirá siendo secreta hasta que alguien más la descubra. Este es el caso de las vulnerabilidades que la NSA explota para sus escuchas y las que explota el Comando Cibernético de Estados Unidos para su armamento ofensivo. Al final, el proveedor del software afectado se entera de la vulnerabilidad (el momento depende de cuándo y cómo se use) y publica un parche para solucionarla.

Los descubridores pueden vender esas vulnerabilidades de día cero. Hay un rico mercado para estos fines de ataque: tanto criminales en el mercado negro[3] como Gobiernos.[4] Las compañías como Azimuth solo venden vulnerabilidades y herramientas de piratería a las democracias;[5] otros muchos son menos exigentes. Y aunque los proveedores ofrezcan recompensas por vulnerabilidades para motivar su divulgación, no pueden igualar las que ofrecen los delincuentes, los Gobiernos y los fabricantes de armas cibernéticas.[6] Un ejemplo: el Proyecto Tor sin ánimo de lucro ofrece cuatro mil dólares por encontrar vulnerabilidades en su navegador anónimo,[7] mientras que el fabricante de ciberarmas Zerodium pagará 250.000 dólares por una vulnerabilidad explotable de Tor.[8]

Volviendo a la doble misión de la NSA, esta puede jugar a la defensa o al ataque. Si la NSA encuentra una vulnerabilidad, puede alertar al proveedor y arreglarla mientras sea secreta, o conservarla y usarla para vigilar sistemas informáticos extranjeros. Corregir la vulnerabilidad fortalece la seguridad de Internet contra todos los atacantes: otros países, delincuentes o piratas informáticos. Al dejar abierta la vulnerabilidad el organismo es más capaz de atacar a otros. Pero con cada uso se corre el riesgo de que el Gobierno

objetivo la descubra y la utilice, o que se haga pública y la usen los delincuentes. Como dijo Jack Goldsmith, profesor de Derecho de Harvard, «cada arma ofensiva es un problema (potencial) en nuestra defensa, y viceversa».[9]

Muchas personas han intervenido en este debate.[10] El activista y escritor Cory Doctorow lo llama problema de salud pública;[11] yo he dicho cosas similares.[12] El experto en seguridad informática Dan Geer recomienda que el Gobierno de Estados Unidos acapare el mercado de vulnerabilidades y las arregle todas.[13] Tanto Brad Smith[14] como Mozilla[15] de Microsoft han hablado sobre esto y han exigido más comunicación sobre vulnerabilidades por parte de los Gobiernos.

El Grupo de Revisión para Tecnologías de Inteligencia y Comunicaciones del presidente Obama, convocado después del caso Snowden, concluyó que las vulnerabilidades solo deberían atesorarse en casos excepcionales y durante períodos cortos:

> Recomendamos que el personal del Consejo de Seguridad Nacional dirija un proceso interinstitucional para revisar periódicamente las actividades del Gobierno de Estados Unidos con respecto a los ataques que explotan una vulnerabilidad desconocida en una aplicación o sistema de ordenadores. La política de Estados Unidos sobre los días cero debe asegurar que se bloqueen rápidamente, por lo que las vulnerabilidades subyacentes deben ser parcheadas por el Gobierno y otras redes. En raras ocasiones, las políticas de Estados Unidos pueden autorizar brevemente el uso de un día cero para la recopilación de información de prioridad alta después de una revisión interinstitucional de alto nivel que involucre a todos los departamentos competentes.[16]

La razón por la que estos argumentos no son convincentes es la carrera de armamentos en la guerra cibernética de la que hablaba en el capítulo 4. Si abandonamos nuestras propias capacidades ofensivas para hacer que Internet sea más seguro, esto equivaldría a un desarme unilateral.[17] Así habló al respecto en 2017 el ex director adjunto de la NSA Rick Ledgett:

> La idea de que estos problemas serían resueltos por el Gobierno de Estados Unidos y que este revelaría cualquier vulnerabilidad en su poder es, en el mejor de los casos, ingenua y, en el peor, peligrosa. Dicha divulgación sería equivalente a un desarme unilateral en un área donde Estados Unidos no puede permitirse estar desarmado […]. Y esta

> no es un área en la que el liderazgo estadounidense haría que otros países cambiaran sus actitudes. Ni nuestros aliados ni nuestros adversarios revelarían las vulnerabilidades en su poder.[18]

Además, no todas las vulnerabilidades son iguales. Algunas son lo que la NSA llama NOBUS[19] (*nobody but us*, que significa «nadie excepto nosotros»), destinado a designar una vulnerabilidad que Estados Unidos haya encontrado y que pueda explotar, pero que nadie más pueda hacerlo porque requiera más recursos que los que tienen otros, o su descubrimiento se basa en un conocimiento especializado que nadie más posee, o su uso requiere una tecnología única con la que nadie más cuenta. Si una vulnerabilidad es NOBUS, la discusión continúa, y Estados Unidos puede reservarla para la ofensa porque nadie más puede usarla contra nosotros.[20]

Este enfoque parece sensato en apariencia, pero los detalles se convierten rápidamente en un embrollo. En Estados Unidos, la decisión acerca de si divulgar o utilizar una vulnerabilidad tiene lugar durante lo que se denomina *proceso de acciones de vulnerabilidad* (PAV), un proceso secreto llevado a cabo por organismos que consideran diferentes valores; es decir, las razones para mantener en secreto esa vulnerabilidad. En 2014, el coordinador de ciberseguridad de la Casa Blanca Michael Daniel escribió una explicación pública sobre el PAV que carecía de detalles reales;[21] en 2016, se publicó el documento oficial de la Casa Blanca, redactado con esmero, donde se establecía la política,[22] y, en 2017, el nuevo coordinador de ciberseguridad Rob Joyce publicó una política revisada sobre el PAV con algunos detalles más;[23] así que tenemos algunas pistas, pero aún no tenemos suficiente información como para juzgar adecuadamente esta política.

No sabemos cómo decide el Gobierno qué divulgar y qué almacenar. Lo que sabemos es que solo las organizaciones con diferentes intereses en una vulnerabilidad particular opinan sobre si esta se mantiene en secreto o no. Parece que no hay nadie involucrado en el PAV que defienda en especial una mayor seguridad mediante la divulgación y, además, los ciudadanos particulares, preocupados por proteger los datos en riesgo de una vulnerabilidad determinada, no están representados.

Es inevitable que el PAV dé como resultado la no divulgación de vulnerabilidades con un potencial ofensivo poderoso sin importar el riesgo que estas supongan. Por ejemplo, Eternal Blue, la vulnerabilidad crítica de Windows que los rusos le robaron a la NSA y que luego publicaron en 2017, se consideró adecuada para la acumulación, y no para la divulgación.[24] Esto

es una locura. Cualquier proceso que permita que una vulnerabilidad grave en un sistema tan ampliamente utilizado permanezca sin parchear durante más de cinco años no está sirviendo muy bien a la seguridad.[25]

Esto plantea la preocupación de que el PAV esté llevando a una acumulación de vulnerabilidades mucho mayor de lo que se considera prudente. Las vulnerabilidades se descubren de forma independiente por azar mucho más a menudo de lo que cabría esperar.[26] La razón parece ser que ciertos tipos de investigación están de moda, y a menudo múltiples grupos de investigación están centrados en las mismas áreas. Esto implica que, si el Gobierno de Estados Unidos descubre una vulnerabilidad, existe una posibilidad razonable de que otra persona la descubra por otro lado.[27] Además, NOBUS no tiene en cuenta que los países se roban vulnerabilidades unos a otros, como Eternal Blue. Tanto la NSA como la CIA han tenido herramientas de ataque cibernético, también vulnerabilidades de día cero, robadas y publicadas,[28] incluyendo algunas de Windows bastante desagradables que la NSA había estado explotando durante años.[29] Tal vez nadie más pudiera haberlas descubierto de manera independiente, pero eso no importó cuando fueron robadas y publicadas.[30]

Tampoco sabemos cuántas vulnerabilidades atraviesan este proceso. En 2015, nos enteramos de que el Gobierno de Estados Unidos revela el 91 % de las vulnerabilidades que descubre, aunque no está claro si esta cifra se refiere a aquellas explotables o si el porcentaje está cubierto por un número mucho mayor de las totales.[31] Sin conocer el denominador común, la estadística no tiene sentido.

Mis ideas son similares a las de Jason Healey:

> Cada año, el Gobierno guarda un número muy pequeño de días cero, tal vez de solo un dígito. Además, estimamos que el Gobierno probablemente retenga un pequeño arsenal de docenas de esos días cero, mucho menos que los cientos o miles que muchos expertos han estimado. Parece que el Gobierno de Estados Unidos suma cifras a ese arsenal con cuentagotas, quizá de un único dígito cada año.[32]

A fin de cuentas, ni siquiera sabemos qué clase de vulnerabilidades siguen el proceso y cuáles no. Parece como si todas las que ha descubierto el Gobierno, probablemente casi en su totalidad la NSA, pasaran por el proceso, pero no aquellas compradas a terceros o las que se basan en decisiones de diseño incorrectas, como tener una contraseña predeterminada. ¿Qué pasa con las

vulnerabilidades que la NSA encuentra después de infiltrarse en redes extranjeras y robar sus armas cibernéticas? No lo sabemos.

En cambio, sí sabemos que las vulnerabilidades se reevalúan cada año, y eso es bueno. Y por mucho que quiera que el PAV de Estados Unidos mejore, al menos cuenta con un proceso. Ningún otro país tiene algo similar, por lo menos público. Muchos otros países nunca revelarían vulnerabilidades para mejorar la seguridad cibernética del mundo. No sabemos nada sobre los países europeos, aunque sé que Alemania está trabajando en algún tipo de política de divulgación.

Hay más problemas que afectan el PAV. Las armas cibernéticas son la combinación de una carga útil (el daño que hace el arma) y un mecanismo de entrega (la vulnerabilidad utilizada para llevar la carga útil hasta la red enemiga). Imagina que China conoce una vulnerabilidad y la utiliza en un arma cibernética que aún no ha disparado, y que la NSA se entera de ella mediante el espionaje. ¿Debería la NSA divulgar y parchear la vulnerabilidad o acumularla para un ataque? Si la revela, desactivaría el arma de China, pero China podría encontrar una vulnerabilidad de reemplazo que la NSA no conozca. Si la acumula, está haciendo a propósito que Estados Unidos sea vulnerable al ataque cibernético. Tal vez algún día lleguemos a un punto en el que podamos parchear las vulnerabilidades más rápido de lo que el enemigo pueda usarlas en un ataque, pero hoy no estamos ni siquiera cerca.

Una vulnerabilidad sin parches nos pone a todos en riesgo, pero no de manera uniforme. Estados Unidos y otros países occidentales están en alto riesgo debido a la infraestructura electrónica crítica, la propiedad intelectual y la riqueza personal. Los países como Corea del Norte corren mucho menos riesgo, por lo que tienen menos alicientes para corregir vulnerabilidades. Arreglar una vulnerabilidad no significa desarmarse; es algo que hace que nuestros propios países sean mucho más seguros. También recuperamos la autoridad moral para negociar amplias reducciones internacionales en las armas cibernéticas y podemos decidir no usarlas incluso aunque otros lo hagan.

Para muchos observadores, está claro que el PAV no funciona.[33] A pesar del intento de transparencia de Joyce, no hay manera de que la gente juzgue su eficacia. Por lo que podemos deducir de los resultados, este proceso secreto no está generando un equilibrio entre los distintos intereses; al contrario, nos está haciendo mucho menos seguros.[34]

Rick Ledgett tiene razón en que nuestros enemigos seguirán acumulando vulnerabilidades, con independencia de lo que decidamos hacer. Pero, si

elegimos la revelación, suceden cuatro cosas: una, las vulnerabilidades que divulguemos se arreglarán en algún momento y privarán a todos de ellas; dos, la seguridad mejorará a medida que todos aprendamos de las vulnerabilidades que se encuentren y se revelen; tres, estableceremos un ejemplo para otros países y luego podremos comenzar a cambiar las normas globales, y cuatro, una vez que organizaciones como la NSA y la CIA renuncien por propia voluntad a estas herramientas de ataque, podremos situar a estos organismos firmemente del lado de la defensa y en contra de la ofensiva, y cuando esto suceda, podremos avanzar hacia una seguridad de Internet+ para todos.

DISEÑO PARA LA SEGURIDAD, Y NO PARA LA VIGILANCIA

No solo es necesario encontrar fallos de seguridad en los sistemas de software existentes. Con demasiada frecuencia, los Gobiernos intervienen en los estándares de seguridad, no para garantizar que sean fuertes, sino para debilitarlos. Es decir, priorizan la ofensiva sobre la defensa.

Por ejemplo, IPsec es un estándar de cifrado y autenticación para paquetes de datos de Internet. Fue por la década de 1990 cuando el Grupo de Trabajo de Ingeniería de Internet (que es el grupo público de estándares de múltiples partes interesadas por Internet) debatió estos estándares, diseñados para defenderse contra un amplio espectro de ataques. La NSA participó en el proceso y trabajó deliberadamente para hacerlo menos seguro;[35] en concreto, trató de hacer cambios menores que debilitaran la seguridad, impulsó un estándar de cifrado entonces débil, exigió una opción de no cifrado, retrasó el proceso de varias maneras y, en general, hizo el estándar tan complejo que cualquier implementación se volvió difícil e insegura. Yo evalué el estándar en 1999 y llegué a la conclusión de que su innecesaria complejidad tenía un efecto devastador en la seguridad.[36] Hoy en día, el cifrado de extremo a extremo aún no está generalizado en Internet.

Un segundo ejemplo: en el proceso solo para Gobiernos de normas secretas para el cifrado digital móvil, muchos creen que la NSA se aseguró de que los algoritmos utilizados para cifrar el tráfico de voz entre los teléfonos y la torre fueran fáciles de romper y de que no hubiera un cifrado de extremo a extremo entre las dos partes que se comunican.[37] El resultado es que tus conversaciones por teléfono móvil pueden controlarse con facilidad.

Ambas cosas probablemente formaban parte del programa Bullrun de la NSA, cuyo objetivo era debilitar los estándares de seguridad pública.[38] (El

programa análogo del Reino Unido se llamaba Edgehill). Y, en ambos casos, los Gobiernos extranjeros y los criminales utilizaron los protocolos de comunicaciones inseguras resultantes para espiar las comunicaciones de ciudadanos particulares.

A veces, el Gobierno debilita la seguridad por ley. La Ley de Asistencia de Comunicaciones para la Aplicación de la Ley (CALEA, por sus siglas en inglés) es una ley de 1994 que obligaba a las compañías telefónicas a incluir funciones de escucha telefónica en sus centralitas para que el FBI pudiera espiar a los usuarios de teléfono.[39] Avanzando hasta el día de hoy, el FBI y sus equivalentes en muchos otros países exigen puertas traseras similares para ordenadores, teléfonos y sistemas de comunicaciones. (Veremos más sobre esto en el capítulo 11).

Y, a veces, el Gobierno de Estados Unidos no tiene que debilitar a propósito los estándares de seguridad, sino que en ocasiones estos se diseñan de manera insegura por otras razones y el Gobierno se aprovecha de ello, mientras que al mismo tiempo oculta el hecho y retrasa los intentos de proteger esos sistemas.

Stingray («mantarraya») es ahora un nombre genérico para un receptor IMSI, que es básicamente una torre de teléfono móvil falsa originalmente vendida por Harris Corporation (como StingRay) a varios organismos de seguridad. (En realidad es solo uno más de una serie de dispositivos con nombres de peces, como Amberjack [«pez limón»],[40] pero es como se conoce en los medios de comunicación). En esencia, un Stingray engaña a los teléfonos móviles cercanos para que se conecten a él. La tecnología funciona porque el teléfono de tu bolsillo confía en cualquier torre de telefonía dentro de su alcance. No hay autenticación en los protocolos de conexión entre los teléfonos y las torres, sino que, cuando aparece una nueva, tu teléfono transmite automáticamente su identidad de abonado móvil internacional (IMSI, por sus siglas en inglés), un número de serie único que le permite al sistema móvil saber dónde te encuentras, lo que hace posible la recopilación de información de identificación y ubicación de los teléfonos en las proximidades y, en algunos casos, la interceptación de conversaciones telefónicas, mensajes de texto y navegación web.[41]

El uso de receptores de IMSI por parte del FBI y otros organismos policiales en Estados Unidos era un enorme secreto. Hace solo unos años, el FBI tenía tanto miedo de explicar este hecho en público que hizo que los departamentos de policía locales firmaran acuerdos de confidencialidad antes de usar la técnica y les ordenó que mintieran sobre su uso en los tribunales.[42]

Cuando parecía que la policía local de Sarasota (Florida) iba a divulgar documentos sobre los receptores de IMSI a los demandantes en los litigios de derechos civiles en su contra, los agentes federales se apoderaron de los documentos.[43] Incluso después de que la tecnología fuera de conocimiento general, y en un punto clave de la trama en programas de televisión, como *The Wire*, el FBI continuó fingiendo que era un gran secreto. En 2015, la policía de St. Louis abandonó un caso para no tener que hablar sobre esta tecnología en los tribunales.[44]

Las compañías de móviles podrían incluir cifrado y autenticación en sus estándares, pero, mientras la mayoría de las personas no entiendan la desprotección de sus teléfonos y los estándares solo dependan del Gobierno, es algo poco probable.

El argumento de NOBUS es de este estilo. Cuando se diseñó la red de telefonía móvil, instalar una torre de telefonía era un ejercicio técnico muy difícil y era razonable suponer que solo lo harían los proveedores legales de móviles. Con el tiempo, la tecnología se volvió más barata y más sencilla. Lo que alguna vez fue un programa secreto de interceptación de la NSA y una herramienta de investigación secreta del FBI se convirtió en utilizable por Gobiernos, ciberdelincuentes e incluso aficionados menos capaces.[45] En 2010, los piratas informáticos enseñaban sus receptores de IMSI de fabricación casera en conferencias.[46] Para 2014, se descubrieron decenas de receptores de IMSI en el área de Washington que recopilaban información sobre quién conoce a quién, y gestionados por quién sabe qué Gobierno u organización criminal.[47] Ahora puedes entrar en la web de comercio electrónico chino Alibaba.com y comprar tu propio receptor IMSI por menos de dos mil dólares[48] o descargarte el software de dominio público que convertirá tu ordenador portátil en uno con los periféricos adecuados.

Otro ejemplo: los sistemas de interceptación de IP se utilizan para espiar lo que las personas hacen en Internet. A diferencia de la vigilancia de compañías como Facebook y Google, que tiene lugar en los sitios que visitas, o la vigilancia en la red troncal de Internet, esta se produce cerca del punto en que tu ordenador se conecta a Internet. Aquí, alguien puede escuchar todo lo que haces.

Los sistemas de interceptación de IP también explotan las vulnerabilidades existentes en los protocolos de comunicaciones de Internet subyacentes. La mayor parte del tráfico entre tu ordenador e Internet no está cifrado, y, aunque lo esté, a menudo es vulnerable a los ataques de

intermediarios debido a las inseguridades en los protocolos de Internet y en los protocolos de cifrado que lo protegen.

Sabemos por los documentos de Snowden que la NSA realiza amplias operaciones de recolección de datos en la red troncal de Internet y se beneficia directamente de la falta de cifrado en la Red.[49] Pero también lo hacen otros países, ciberdelincuentes y hackers.

De manera similar, cuando los protocolos de Internet se diseñaron por primera vez, la incorporación de cifrado habría ralentizado bastante aquellos primeros ordenadores, por lo que parecía un desperdicio de recursos. Ahora los ordenadores son baratos y el software es rápido, y es fácil lo que era difícil o imposible hace solo unas décadas. Al mismo tiempo, las capacidades de vigilancia de Internet que alguna vez fueron exclusivas de la NSA se han vuelto tan accesibles que los delincuentes, los piratas informáticos y los servicios de inteligencia de cualquier país pueden emplearlas.

No hay una gran diferencia con el cifrado de teléfonos móviles o los sistemas de escuchas telefónicas estipulados por CALEA. Esa misma capacidad fue utilizada por atacantes desconocidos a través de centralitas para pinchar los teléfonos de más de cien miembros del Gobierno griego en el transcurso de diez meses a principios del 2000.[50] CALEA causó de manera inadvertida vulnerabilidades en los interruptores de Internet de Cisco.[51] Y según Richard George, el antiguo director técnico de la NSA para el Aseguramiento de la Información, «cuando la NSA probó las centralitas compatibles con CALEA que se habían enviado antes de su uso en los sistemas DoD, la NSA encontró problemas de seguridad en cada una que era enviada para la prueba».[52]

En cada una de estas historias la lección es la misma: NOBUS no dura. Incluso el exdirector de la NSA y la CIA Michael Hayden, quien popularizó el término en la prensa pública,[53] escribió en 2017 lo siguiente: «La zona de confort de NOBUS es considerablemente más pequeña de lo que alguna vez fue».[54] En un mundo donde todos usan los mismos ordenadores y sistemas de comunicación, cualquier inseguridad que introducimos a propósito —o incluso la que encontremos y utilicemos convenientemente— puede y será utilizada en nuestra contra. Y, de la misma manera que arreglando las vulnerabilidades, estaríamos mucho más seguros si nuestros sistemas se diseñaran para ser seguros en primer lugar.

CIFRAR TANTO COMO SEA POSIBLE

Los Gobiernos deben tener el objetivo de cifrar Internet+ lo máximo posible, aunque cabe considerar diferentes aspectos.

Primero, necesitamos cifrado de extremo a extremo para las comunicaciones, lo que significa que todas deben estar encriptadas desde el dispositivo del emisor hasta el del receptor, y que nadie en el medio debe poder leer esa comunicación. Este es el tipo de cifrado utilizado por muchas aplicaciones de mensajería, como iMessage, WhatsApp y Signal, y también de tu navegador. Pero, en algunos casos, no es deseable el auténtico cifrado de extremo a extremo. La mayoría de nosotros queremos que Google pueda leer nuestro correo electrónico porque así es como lo clasifica en carpetas y elimina el no deseado, por lo que, en estos casos, debemos cifrar las comunicaciones hasta nuestro procesador de comunicaciones designado (y en teoría fiable).

En segundo lugar, tenemos que cifrar nuestros dispositivos. El cifrado aumenta en gran medida la seguridad de cualquier dispositivo de usuario final, pero es importante sobre todo para aquellos de uso general, como ordenadores y teléfonos, ya que a menudo son núcleos centrales en nuestra vida de Internet+ y deben ser lo más seguros posible.

En tercer lugar, necesitamos encriptar Internet. Los datos deben cifrarse siempre que sea posible a medida que se mueven por Internet. Por desgracia, todos nos hemos acostumbrado a un Internet sin cifrar y hay muchos protocolos que demuestran este hecho. Cuando te conectas a una red wifi extraña, lo que suele suceder es que el rúter intercepta tu navegación y la página que deseas ver es reemplazada por una pantalla de inicio de sesión. Eso sucede porque tus datos no están cifrados. A pesar de que esta característica aprovecha las comunicaciones no cifradas, necesitamos cifrarlas de todas formas y desarrollar otras maneras de iniciar sesión.

Y cuarto, necesitamos encriptar las grandes bases de datos de información personal que están disponibles.

El cifrado no es la panacea. Los ataques contra el sistema de autenticación a menudo se saltan el cifrado robando la contraseña de un usuario autorizado, y la encriptación tampoco impedirá el espionaje entre Gobiernos. Todas las lecciones del capítulo 1 siguen vigentes: los ordenadores son muy difíciles de proteger. Sabemos que la NSA es capaz de eludir la mayoría de los cifrados al atacar el software subyacente, pero se trata de ataques más dirigidos.

Un sistema de comunicaciones cifrado —un ordenador— no es seguro hasta el punto de ser impenetrable, y uno sin cifrado no tiene por qué ser inseguro de forma permanente. Pero la encriptación es una tecnología de

seguridad central: protege nuestra información y dispositivos de hackers, delincuentes y Gobiernos extranjeros; además de protegernos de la vigilancia de nuestros propios Gobiernos, protege a nuestros funcionarios electos de escuchas ilegales y evita que nuestros dispositivos del IoT sean alterados, y cada vez más protege nuestra infraestructura crítica. Combinada con la autenticación es probablemente la característica más esencial de seguridad para Internet+. Muchos fallos de seguridad pueden atribuirse a la falta de cifrado.

La encriptación generalizada obliga al atacante a dirigir sus ataques, debido a que hace que la vigilancia masiva sea imposible en muchos casos. Esto afecta a la vigilancia del Gobierno sobre la población mucho más que al espionaje de un Gobierno a otro, y perjudica mucho más a los Gobiernos represivos que a las democracias. El cifrado es beneficioso para la sociedad, aunque los malhechores pueden usarlo para proteger sus comunicaciones y dispositivos, igual que cualquier otra persona.

No se trata de una postura universal. Existe una fuerte presión para debilitar el cifrado, no solo por parte de los Gobiernos totalitarios que quieren espiar a sus ciudadanos, sino también de los políticos y los funcionarios encargados de hacer cumplir la ley en las democracias, que ven el cifrado como una herramienta utilizada por criminales, terroristas y, con la llegada de las monedas virtuales, por gente que quiere comprar drogas y lavar dinero.

Muchos tecnólogos de seguridad y yo hemos argumentado que el requerimiento de puertas traseras del FBI es demasiado peligroso.[55] Por supuesto, los delincuentes y los terroristas han utilizado, están utilizando y seguirán utilizando el cifrado para ocultar sus tramas a las autoridades, del mismo modo que se aprovecharán de muchos otros aspectos de las capacidades y de la infraestructura de la sociedad. En general, reconocemos que los coches, los restaurantes y las telecomunicaciones pueden ser utilizados por personas honestas y deshonestas; sin embargo, la sociedad prospera porque los honestos superan en gran medida a los que no lo son. A modo de experimento mental, compara la idea de las puertas traseras con la de incorporar un regulador de velocidad a cada motor de automóvil para asegurar que nadie acelere nunca. Sí, eso ayudaría a evitar que los criminales usaran automóviles para escapar, pero nunca aceptaríamos la carga para los ciudadanos honestos. El debilitamiento del cifrado para todos es perjudicial de la misma manera, incluso aunque los efectos no sean tan obvios. Hablaremos más sobre esto en el capítulo 11.

SEGURIDAD SEPARADA DEL ESPIONAJE

La misión dual de la NSA no solo es contraria a sí misma, sino que no tiene sentido organizativo. La ofensa recibe el dinero, la atención y la prioridad. Mientras la NSA sea responsable tanto de la ofensiva como de la defensa, nunca se confiará por completo en la seguridad de Internet+. Esto significa que esa organización, tal y como está constituida en la actualidad, es perjudicial para la ciberseguridad.

Necesitamos organismos gubernamentales sólidos del lado de la seguridad, lo que significa separarse de la NSA y financiar significativamente iniciativas defensivas. En *Data y Goliat* recomendaba dividir la NSA en tres organizaciones: una que lleve a cabo el espionaje electrónico internacional, otra que proporcione seguridad en el ciberespacio y la última, incorporada al FBI, que lleve a cabo la vigilancia doméstica legal. Si la organización de seguridad pudiera trabajar estrechamente, o incluso formar parte de la agencia reguladora de Internet+ descrita en el capítulo 8, ayudaría a que el mundo fuera más seguro.

Lo mismo sucede en otros países. Siempre y cuando el Centro Nacional de Seguridad Cibernética del Reino Unido esté al servicio de GCHQ (es decir, de la Sede de Comunicaciones del Gobierno, la agencia de vigilancia del país), nunca se podrá confiar en él.[56] Un modelo mejor es el de Alemania. La Oficina Federal Alemana para la Seguridad de la Información (BSI, por sus siglas en inglés) informa al canciller mediante un ministro diferente al del Servicio Federal de Inteligencia (BND, por sus siglas en inglés), su agencia ofensiva.

Separar la seguridad del espionaje (y también del ataque) tiene otros beneficios. Revelar vulnerabilidades es muy difícil para una organización que también quiere usarlas de manera ofensiva. Evidentemente, a los dos organismos se les pueden asignar diferentes cantidades de financiación, pero al menos ese proceso es público y está sujeto a cierto escrutinio. En general, la separación reduciría el secretismo que rodea hoy en día todo lo que concierne a la seguridad del Gobierno en el ciberespacio y que tiene que ver sobre todo con las capacidades y las misiones ofensivas.

Menos secretismo también significa más supervisión, y ese es un problema clave con organismos como la NSA. Cuanto más se debatan en público sus autoridades, capacidades y programas, menos probabilidades hay de que sean objeto de abuso.

Por desgracia, en 2016, la NSA experimentó una importante reorganización en la que combinó sus capacidades ofensiva y defensiva en

una única dirección operativa.[57] Si bien esto tiene mucho sentido desde el punto de vista técnico, se requieren las mismas habilidades y experiencia para ambas, y es justo lo contrario de lo que necesitamos políticamente. Si alguna vez se confía en la NSA para proteger Internet+ en lugar de atacarlo, la defensa no puede mezclarse con la ofensiva.[58] Así como la inteligencia y las capacidades de ataque son ahora organizaciones separadas (la NSA y el Cibercomando de Estados Unidos, respectivamente), la defensa y la ofensiva también deben serlo, aunque las habilidades y la experiencia sean las mismas.

HACER QUE LA APLICACIÓN DE LA LEY SEA MÁS INTELIGENTE

Si vamos a darle prioridad a la defensa sobre la ofensiva, tendremos que reconocer el desafío que esto supone para la aplicación de la ley. El FBI necesita capacidades de investigación adecuadas para el siglo XXI.

En 2016, el FBI exigió que Apple desbloqueara un iPhone perteneciente al terrorista muerto de San Bernardino Syed Rizwan Farook. Apple tiene implementado el cifrado en los teléfonos de forma predeterminada y el FBI no pudo acceder a los datos, pero, debido a que era un iPhone 5C, la empresa sí tenía acceso a ellos.[59] (Apple mejoró la seguridad de los modelos de iPhone posteriores). Apple se opuso a la petición del FBI, principalmente porque reconoció que era una prueba de la capacidad del organismo para forzarla (y a cualquier compañía de tecnología) a pasar por alto la seguridad de sus sistemas y dispositivos.[60]

Es la misma solicitud de puerta trasera que hemos escuchado del FBI durante décadas, y hablaremos más sobre esto en el capítulo 11. Para el FBI, este era un buen precedente y pensó que ganaría en los tribunales con facilidad. Apple, junto con casi todos los profesionales de la ciberseguridad, se defendió. Al final, el FBI consiguió que un tercero no identificado, probablemente la compañía israelí Cellebrite,[61] accediera al teléfono sin la ayuda de Apple.[62] Ningún tribunal decidió nada.

Después de que todo terminara, un grupo de colegas y yo escribimos un artículo sobre este tema con el título «Don’t Panic» («No te asustes»).[63] El título era literal. El FBI y otros más debían dejar de asustarse por el cifrado. Esto no significa que los delitos se vuelvan de pronto irresolubles porque el FBI no pueda extraer datos de los ordenadores o escuchar las comunicaciones, teniendo en cuenta que la delincuencia tenía solución antes

de que nosotros usáramos los ordenadores o nos comunicáramos digitalmente. Dimos tres razones principales para no entrar en pánico:

1. Los metadatos no pueden cifrarse, ya que deben permanecer en una forma utilizable dentro de la red. La policía siempre puede saber quién está hablando con quién, dónde y cuándo, incluso aunque no sepan exactamente lo que se dice.

2. Cuando la gente utiliza a terceros para el almacenamiento y procesamiento de datos, esos datos no pueden cifrarse. Incluso las empresas que proporcionan almacenamiento de datos encriptados a menudo permiten recuperar archivos, porque eso es lo que la mayoría de los usuarios demanda. Todos esos datos estarán siempre disponibles con una orden de registro, y en algunos casos sin ella.

3. Si todo se está convirtiendo en un ordenador, entonces todo se está convirtiendo en un posible dispositivo de vigilancia. En concreto, todos los nuevos sensores que alimentan el Internet de las cosas proporcionarán a la policía nuevas y vastas transmisiones de datos que no estarán cifrados de extremo a extremo, lo que permitirá tanto la vigilancia en tiempo real como el acceso posterior al hecho.

Lo cierto es que el FBI ha perdido gran parte de su experiencia técnica. Antes de que existieran los teléfonos móviles, cuando las conversaciones de las personas se evaporaban sin remedio tan pronto como se pronunciaban las palabras, el FBI tenía todo tipo de técnicas de investigación que podían aplicarse a un crimen sin resolver. Desde mediados de la década de 1990, su trabajo se hizo más fácil: obtener los datos de los teléfonos móviles. Ahora, más de veinte años después, esa época está llegando a su fin, pero todos los agentes del FBI que recuerdan los viejos tiempos se han retirado. Lo único que tiene este organismo son personas que saben que hay datos importantes en los teléfonos inteligentes.[64]

Esto tiene que cambiar. Si vamos a hacer lo correcto y colocar sistemas de seguridad ubicuos sin ningún tipo de puertas traseras, el FBI necesita nuevos conocimientos sobre cómo llevar a cabo investigaciones en la era de Internet+. En su testimonio ante el Comité Judicial de la Cámara de Representantes, la matemática y experta en política de seguridad cibernética Susan Landau describió lo siguiente:

> El FBI necesitará un centro de investigación con agentes dotados con un profundo conocimiento técnico de las modernas tecnologías en telecomunicaciones; desde la capa física hasta la virtual y todas las piezas intermedias. Dado que en estos días todos los teléfonos son

> ordenadores, este centro deberá tener el mismo nivel de experiencia profunda en informática. Además, será necesario que haya equipos de investigadores que comprendan los distintos tipos de dispositivos de campo. Esto incluirá no solo dónde está y estará en seis meses la tecnología, sino dónde puede estar en dos o cinco años. Este centro deberá realizar investigaciones sobre qué nuevas tecnologías de vigilancia deberán desarrollarse como resultado de las direcciones de esas nuevas tecnologías. Estoy hablando de un gran conocimiento y de una gran aptitud, no de algo sin importancia.[65]

Hay demasiadas piezas aquí. Además de mejorar la informática forense, el FBI necesita aptitudes legales de piratería que pueda usar en circunstancias excepcionales[66] y también debe proporcionar asistencia técnica a los organismos estatales y locales encargados de hacer cumplir la ley, que se enfrentan a las mismas dificultades con la tecnología forense y la recopilación de pruebas. Este problema no va a desaparecer, sino que cambiará con el tiempo, por lo que el FBI necesitará adaptarse continuamente.

Para que esto suceda, el FBI debe establecer una trayectoria profesional viable para los investigadores técnicos. En este momento no hay ninguna, y sería difícil encontrar un estudiante en el campo de las ciencias de la computación pensando en seguir una carrera policial. Es por esto por lo que los expertos en informática forense del FBI tienden a proceder de fuera del campo. Si el FBI va a atraer y retener al mejor talento, tendrá que competir con éxito con el sector privado.[67]

Esto no será barato. Landau estima que costará cientos de millones de dólares cada año, pero es mucho menos que los miles de millones de dólares que la inseguridad de Internet+ le costará a la sociedad, y en realidad es la única solución que puede funcionar.

REPENSAR LA RELACIÓN ENTRE EL GOBIERNO Y LA INDUSTRIA

El Gobierno no puede hacer esto solo. El sector privado no puede hacer esto solo. Cualquier solución real requiere que el Gobierno y la industria trabajen juntos.

Muchas de las recomendaciones de los capítulos anteriores tratan de delinear los contornos de esa posible asociación. Ya sean proveedores de

software, empresas de Internet, fabricantes del IoT o proveedores de infraestructura crítica, las empresas deben comprender sus responsabilidades.

Esto significa más intercambio de información entre el Gobierno y el sector privado. No es una idea nueva; los últimos cuatro presidentes de Estados Unidos lo han intentado. La mayoría de los sectores de la industria crítica tienen sus propios centros de análisis e intercambio de información en los que el Gobierno y las empresas pueden compartir información de inteligencia. Otros países tienen organizaciones similares: el Centro para la Protección de la Infraestructura Nacional del Reino Unido, el Centro de Análisis e Intercambio de Información Energética de la UE, el Grupo Trabajo Seguridad español y la Red de Intercambio de Información Fiable de Australia para Infraestructura Crítica.

La realidad siempre se queda corta, porque tanto el gobierno como la industria tienden a preferir recibir información antes que darla,[68] lo cual es algo lógico: los costes y las obstáculos existentes a menudo superan las ventajas.[69]

Gran parte de lo que saben la NSA y el FBI está clasificado, y los organismos no han descubierto cómo compartir sus datos con compañías que carecen de personal con autorización de seguridad. Muchos datos de la industria son vergonzosos o tienen dueño y no se compartirán sin garantías de que no vayan muy lejos. Reducir el secretismo en la ciberseguridad del Gobierno contribuirá en gran medida a facilitar el intercambio de información, al igual que ofrecer algunas garantías de confidencialidad y quizá una compensación a las empresas que compartan información.

Esto es algo más fácil para la infraestructura crítica. Los Gobiernos han estado involucrados durante mucho tiempo en la regulación de estas industrias y tienen experiencia manejando amenazas contra ellas. Sin embargo, el intercambio de información debe extenderse más allá de la típica infraestructura crítica.

Una opción es crear un repositorio nacional de datos sobre incidentes cibernéticos que les permita a las empresas reportar de forma anónima información sobre brechas de seguridad en bases de datos. La FAA mantiene una base de datos anónima de aviones que sufrieron percances que podrían haber sido graves.[70] La notificación es voluntaria pero esperada, y los ingenieros pueden buscar tendencias en la base de datos que los ayuden a construir aviones, pistas de aeropuertos y procedimientos más seguros.

Otra idea es crear una Junta Nacional de Seguridad Cibernética para desastres relacionados con Internet que siga el modelo de la Junta Nacional de

Seguridad del Transporte, el organismo independiente de investigación de accidentes de transporte.[71] Esta junta investigaría los incidentes más graves, facilitaría hallazgos sobre fallos y publicaría información sobre qué medidas de seguridad realmente funcionan (y cuáles no).[72] También podría emitir algo parecido a una lista de los más buscados anual,[73] enumerando los cambios críticos necesarios para prevenir accidentes.[74]

Hagamos lo que hagamos, tendrá que extenderse a Internet+. Por ejemplo, cada vez que un automóvil se estrella, todos querrán tener esa información: la policía de tráfico, las agencias de seguros afectadas, el fabricante de automóviles, el organismo de seguridad local, etc.

Las redes no gubernamentales, como la Cyber Threat Alliance, han surgido para llenar el enorme hueco existente en el intercambio de información fiable.[75] Fue creada en 2014 por cinco proveedores de seguridad con sede en Estados Unidos y se ha expandido rápidamente a nivel mundial. La idea es ayudar a los defensores a adelantarse a los atacantes (abordando algunas de las asimetrías de las que hablábamos en el capítulo 1) al compartir información sobre los métodos y motivos de los ataques. Si bien es vital, este intercambio informal de información no sustituye a los modelos que también incluyen información documentada sobre fallos de seguridad. Las compañías son reacias a compartir esta información entre ellas, lo que habla de la necesidad de un rol del Gobierno para facilitar, o incluso exigir, un mayor intercambio.

También debemos reconocer los límites de cualquier asociación pública o privada y determinar qué hacer cuando los Gobiernos atacan a civiles en Internet. Imagina que los militares de Corea del Norte atacaran físicamente a una compañía de medios de comunicación de Estados Unidos, o que el ejército iraní asaltara un casino estadounidense. No esperaríamos que esas empresas se defendieran, sino que el ejército de Estados Unidos las defendiera, como esperaríamos que hiciera con todos los ciudadanos de Estados Unidos que fueran objeto de ataques extranjeros.

¿Qué sucede si esos dos países atacan a empresas estadounidenses, como de hecho ya ha ocurrido, en el ciberespacio? Con independencia de cuánta información haya compartido el Gobierno con esas compañías, ¿de verdad podemos esperar que Sony se defienda contra Corea del Norte o el casino Sands contra Irán? ¿Acaso queremos que empresas privadas respondan ante un ataque militar extranjero? No lo creo.

Tampoco podemos esperar que empresas como Westinghouse Electric y US Steel se defiendan contra el hackeo militar chino,[76] ni debemos contar

con que los comités nacionales demócratas o republicanos,[77] ni por supuesto las organizaciones políticas estatales y locales, se defiendan contra la piratería del Gobierno ruso. Ninguno de estos casos es una pelea justa.

Uno de los argumentos principales de este libro es que las empresas deben hacer más por proteger sus dispositivos, datos y redes. Esto supondría recorrer un largo camino en la defensa contra las incursiones de Gobiernos extranjeros y dificultaría los ataques exitosos. Ya no es bueno fingir que la amenaza no existe. Al final los militares siempre serán más hábiles y dispondrán de más fondos que los defensores civiles. Siempre habrá ataques que vayan más allá de la capacidad de los defensores civiles para resistirlos. Y el Gobierno deberá seguir siendo el único organismo con autoridad y capacidad para responder a los ataques de los Estados nación a gran escala en el ciberespacio. Tal respuesta puede requerir coordinación y asistencia del sector privado, pero no debe ser responsabilidad exclusiva de este.

Entonces, ¿cuál sería el modelo?, ¿una guardia nacional cibernética?,[78] ¿un grupo cibernético de ingenieros? ¿Esperamos que el Cibercomando de Estados Unidos defienda las redes civiles dentro de Estados Unidos?, ¿o estaría a cargo del Departamento de Seguridad Nacional? Estonia tiene una Unidad de Defensa Cibernética voluntaria formada por expertos no gubernamentales a los que se puede recurrir en momentos de emergencia nacional.[79] No sé si eso es lo que necesitamos aquí, pero sí sé que necesitamos algo.

Sin embargo, cualquier defensa gubernamental organizada contra los ataques de los Estados nación a entidades privadas está muy lejos de ser una realidad. Hasta que llegue ese momento, los individuos y las organizaciones deberán asumir más responsabilidades por su propia seguridad que en cualquier otra época desde el cierre de la frontera estadounidense en 1890.

10

PLAN B: LO QUE PROBABLEMENTE OCURRA

PRIMERA HISTORIA. Tras el ataque a Equifax de 2017 hubo una indignación bipartidista en el Congreso y se habló mucho sobre la regulación de los intermediarios de datos y de aquellos que recopilan y venden nuestros datos personales en general. A pesar de algunas duras palabras, un aluvión de audiencias en el Congreso y varias propuestas, nada salió de aquello.[1] Incluso un proyecto de ley que imponía específicamente la más pequeña de las regulaciones a las agencias de crédito no llegó a ninguna parte.[2] Lo único que hizo el Congreso fue aprobar una ley que impidiera a los consumidores demandar a Equifax.[3]

Segunda historia. La Ley de Mejora de la Ciberseguridad del Internet de las Cosas de 2017 fue una ley modesta:[4] no prescribe, regula ni obliga a ninguna empresa a hacer nada. Impuso estándares mínimos de seguridad en los dispositivos IoT adquiridos por el Gobierno de Estados Unidos. Esos estándares eran razonables y no muy costosos, en la misma línea que discutía en el capítulo 6. El proyecto de ley no fue a ninguna parte, no hubo audiencias y nunca fue votado por ningún comité. Apenas llegó a los periódicos después de su presentación.

Tercera historia. En 2016, el presidente Obama estableció una comisión para mejorar la ciberseguridad nacional.[5] Su competencia fue amplia:

> La Comisión hará recomendaciones detalladas para fortalecer la ciberseguridad tanto en el sector público como en el privado al tiempo que protege la privacidad, garantiza la seguridad pública y la seguridad económica y nacional, fomenta el descubrimiento y el desarrollo de nuevas soluciones técnicas y refuerza las asociaciones entre el Gobierno federal, estatal y local, y el sector privado en el desarrollo, promoción y uso de tecnologías, políticas y mejores prácticas de ciberseguridad. Las recomendaciones de la Comisión deben abordar las acciones que puedan tomarse durante la próxima década para lograr estos objetivos.

A finales de ese año, el grupo bipartidista emitió su informe.[6] Es un buen documento basado en investigaciones sólidas; contiene dieciséis recomendaciones con 53 acciones específicas que la Administración podría hacer para mejorar la seguridad de Internet. Si bien hay cosas con las que no estoy de acuerdo, no era una mala hoja de ruta para la acción inmediata y la planificación de políticas a largo plazo. Casi dos años después, solo una de las recomendaciones se ha convertido en política: hacer que el Marco de Ciberseguridad del NIST sea obligatorio para los organismos gubernamentales.[7] Ningún organismo ha seguido esa política.[8] El resto del informe se ha ignorado.[9]

ESTADOS UNIDOS NO HARÁ NADA PRONTO

Si lees los cuatro capítulos anteriores, es fácil acusarme de pintar una pesadilla y responder con fantasías. Aunque mis recomendaciones pueden ser una buena lista de lo que debemos hacer, no se parecen en nada a lo que haremos.

En parte estoy de acuerdo. No preveo que el Congreso se encargue de las poderosas industrias de ordenadores y de Internet y les imponga estándares de seguridad exigibles, no pronostico ningún aumento del gasto en nuestra infraestructura del ciberespacio, ni la creación de ningún nuevo organismo regulador federal, así como tampoco espero que los militares o la policía abandonen los usos ofensivos del ciberespacio para mejorar la defensa.

Detengámonos ahora un instante en el aspecto psicológico. De la misma manera que los CEO de las empresas tienden a menospreciar la seguridad, los políticos tienden a subestimar las amenazas que no son relevantes de inmediato. Imagina a un político tratando de mitigar un riesgo hipotético a largo plazo mediante una gran asignación presupuestaria. Podría designar fondos para ese propósito o para prioridades políticas más inmediatas. Si hace esto último, es un héroe para sus electores, o al menos los de su partido, mientras que, si se empeña en gastar en seguridad, corre el riesgo de que sus oponentes lo critiquen por desperdiciar dinero o ignorar otras prioridades inmediatas. Esto es peor si la amenaza no se materializa (incluso aunque sea gracias a ese gasto) y aún peor si se materializa cuando la otra facción está en el poder: se atribuirán el mérito de proteger a las personas.

Durante todos los años que llevo escribiendo sobre estos temas he visto un progreso político muy pequeño. Sí he visto, en cambio, a la cada vez más poderosa industria de TI aferrarse y oponerse a cualquier límite

gubernamental con respecto a su comportamiento, y a legisladores sin el estómago para asumirla. He visto a grupos policiales en varios países proponer cambios técnicos que debilitarían la seguridad y que pintaban a cualquiera que se opusiera a ellos como débiles ante el crimen y el terrorismo. He visto al Gobierno acusado de una regulación *al mismo tiempo* excesiva o insuficiente. Y he visto cómo las nuevas tecnologías se convierten en la tendencia dominante sin pensar en la seguridad o en la regulación.

Mientras tanto, los riesgos se han vuelto más graves, las consecuencias más catastróficas y las cuestiones políticas cada vez más difíciles. Internet se ha convertido en una infraestructura crítica; ahora se está volviendo física. Nuestros datos se han trasladado a ordenadores gestionados por otras compañías y nuestras redes se han vuelto globales.

Los Gobiernos regulan las cosas que matan a las personas, y solo cuando Internet comience a matar a gente se regulará. Es cierto que el miedo es un motivador poderoso y puede vencer la propensión psicológica hacia no hacer nada y la inclinación política hacia un Gobierno más pequeño.

¿Cómo sería algo así?

Eso depende del momento. Algunos observadores han señalado paralelismos entre el Internet+ de hoy y la industria automovilística anterior a 1970.[10] Libres de regulaciones, los fabricantes construían y vendían coches inseguros en los que la gente moría. Fue la publicación en 1965 de *Inseguro a cualquier velocidad*, de Ralph Nader, lo que impulsó al Gobierno a actuar y dio como resultado una serie de leyes de seguridad que van desde los cinturones hasta los reposacabezas, etc.[11] Una gran cantidad de muertes relacionadas con Internet+ podrían causar una oleada reguladora similar.

Por otro lado, las empresas han estado matando gente a través del medioambiente durante décadas. Rachel Carson publicó *Primavera silenciosa* en 1962, antes de que se formara en 1970 la Agencia de Protección Ambiental (EPA, por sus siglas en inglés), y casi cincuenta años después sus regulaciones aún son insuficientes para combatir las amenazas. Nunca subestimemos el poder de los grupos de presión de la industria para impulsar sus propias agendas, incluso a expensas del resto del mundo.

La diferencia entre los eventos que provocan reacciones inmediatas y los que tienen consecuencias más a largo plazo podría radicar en la capacidad de conectar una fatalidad con una inseguridad subyacente. Las muertes ambientales son mucho más difíciles de identificar con una causa específica que las producidas por automóviles. Esto también ocurre con Internet. Cuando eres víctima de un robo de identidad, es muy difícil señalar el caso

específico de piratería que lo causó. Incluso cuando hackean una planta de energía y una ciudad se sumerge en la oscuridad, es difícil saber exactamente a qué vulnerabilidad culpar.

No soy optimista a corto plazo. Como sociedad, ni siquiera estamos de acuerdo con ninguna de las grandes ideas. Entendemos los síntomas de inseguridad mejor que los problemas reales, lo que dificulta el análisis de soluciones. No podemos averiguar cuáles deberían ser las políticas porque no sabemos adónde queremos ir. Peor aún, no estamos siquiera teniendo ninguno de estos importantes debates. Dejando a un lado el hecho de obligar a las empresas de tecnología a eliminar el cifrado para satisfacer a las autoridades, la seguridad de Internet+ no es un problema que preocupe a la mayoría de los responsables de las políticas, más allá de dirigirse algunas duras palabras de forma esporádica; no se debate en los medios, no se me ocurre ningún país donde pueda ser un tema de campaña, ni siquiera tenemos un vocabulario común acordado para hablar sobre estos temas.

Compara esto con el blanqueo de dinero, la pornografía infantil o el soborno. Todos estos son grandes problemas internacionales con implicaciones geopolíticas complejas y soluciones políticas matizadas. Pero para esas cuestiones al menos todos estamos de acuerdo sobre en qué dirección queremos que se dirija el mundo. Con la seguridad de Internet+ no estamos ni cerca.

Además, todas las amenazas están mezcladas. *Ciber* es un término general que abarca todo, desde el ciberacoso al ciberterrorismo. Esto podría tener sentido desde un enfoque tecnológico (Internet+ es el aspecto común), pero no lo tiene desde una perspectiva política. El acoso, el delito, la guerra y el terrorismo cibernéticos no son lo mismo, y son diferentes del ciberespionaje y del capitalismo de vigilancia. Unas amenazas son adecuadamente contrarrestadas por la policía o por el ejército, otras no son asunto del Gobierno en absoluto y las combaten con eficacia las partes afectadas, y para responder a algunas debemos hacerlo mediante legislaciones. Del mismo modo que no pensamos en la conducción peligrosa y en los coches bomba de la misma manera, aunque estén involucrados automóviles en ambos casos, no podemos tratar todas las amenazas cibernéticas por igual. No creo que los políticos de Estados Unidos lo entiendan todavía, pero deberán hacerlo si queremos que actúen.

Mi pronóstico es la inactividad legislativa continua a corto plazo en Estados Unidos. Los organismos reguladores, en especial la FTC, continuarán investigando y multando a los infractores más flagrantes. Y no habrá cambios

en la regulación de la vigilancia gubernamental o del capitalismo de vigilancia. Las muertes se atribuirán a individuos y a productos específicos, y no al sistema que las posibilita. A pesar de las amenazas inminentes, creo que la generación más joven llegará al poder antes de que se produzca un cambio real en Estados Unidos.

REGULARÁN OTROS

Hay más esperanzas en Europa. La Unión Europea es el mercado más grande del mundo y se está convirtiendo en una superpotencia reguladora. Y ha estado regulando datos, ordenadores e Internet. El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) supone un cambio radical en la leyes de privacidad;[12] se trata de un amplio reglamento a escala de la UE que afecta a cualquier empresa del mundo que maneje datos personales de ciudadanos de la Unión. La compleja ley se centra sobre todo en los datos y en la privacidad, pero también contiene requisitos para la seguridad del ordenador y de la red. Además, es un plan razonable para lo que la UE podría hacer algún día con respecto a la seguridad de Internet+.

Por ejemplo, el GDPR exige que los datos personales solo se puedan recopilar y guardar con «fines específicos, explícitos y legítimos», y solo con el consentimiento explícito del usuario: el consentimiento no puede sepultarse bajo los términos y condiciones de uso, ni se puede suponer a menos que el usuario lo acepte. Los usuarios tienen derecho a acceder a sus datos personales, corregir información falsa y oponerse a usos concretos de sus datos, así como a descargarlos y utilizarlos en otros lugares o exigir que se borren. Las disposiciones siguen y siguen.[13]

Las regulaciones del GDPR solo afectan a los usuarios y a los clientes de Europa, pero la ley tendrá repercusiones en todo el mundo.[14] Por ejemplo, casi todas las compañías de Internet tienen usuarios europeos, y si sufrieran una filtración de datos, invariablemente tendrían que publicarla con rapidez. Si las empresas tienen que explicarles su recopilación de datos y prácticas de uso a los europeos, todos sabremos cuáles son.[15] Además, las legislaturas de todo el mundo, desde Argentina hasta Colombia y Corea del Sur, están revisando sus leyes de privacidad para garantizar que sean adecuadas para los nuevos estándares de la UE, ya que esta ahora vincula los acuerdos de libre comercio con las regulaciones de privacidad del país aliado.[16]

El GDPR se aprobó en 2016 y entró en vigencia en mayo de 2018, y se espera su aplicación en algún momento de 2019. Las organizaciones ya están

haciendo cosas para que se cumpla la ley, pero en muchos casos esperan a ver cómo será la implementación y el cumplimiento.[17]

Creo que la aplicación de la UE será dura. Las multas pueden llegar al 4 % de los ingresos globales de una empresa.[18] En 2017, vimos varias manifestaciones de que la UE no teme perseguir a las mayores compañías de Internet: multó a Google con 2.500 millones de euros (y amenazó con multar aún más a la compañía con el 5 % de sus ingresos diarios) por la forma en que presentó los resultados de búsqueda para los servicios de compras[19] y, por separado, multó a Facebook con 110 millones de euros por engañar a los reguladores por su capacidad para vincular las cuentas de Facebook y de WhatsApp.[20]

Compara las posibles multas por inseguridad digital en Estados Unidos y en la UE. En 2017, el estado de Nueva York impuso una multa de 700.000 dólares a los hoteles Hilton por dos violaciones en 2015 que involucraban el robo de información personal (incluidos los números de tarjetas de crédito) de 350.000 clientes. Eso son dos dólares por persona para una compañía con 410.000 millones en ingresos, básicamente un error de redondeo. Bajo el GDPR, la multa habría sido de 420 millones de dólares.[21]

La UE también está regulando la seguridad informática de otras maneras. Si te fijas en el envasado de un producto en Europa (y con frecuencia en el resto del mundo) observarás un «ce» en minúsculas en algún lugar de la etiqueta: significa que el producto cumple con todas las normas europeas aplicables, incluida una para la divulgación responsable de vulnerabilidades. Al igual que el GDPR, la marca «ce» solo afecta a los productos vendidos en Europa; no obstante, estas normas se incorporarán a los acuerdos comerciales internacionales, como el Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT, por sus siglas en inglés), y afectarán a los productos en todas partes.

Mi previsión es que la UE centrará su atención en la seguridad y en el Internet de las cosas (IoT) y, en general, en los sistemas cibernéticos. El profesor de la Universidad de Cambridge Ross Anderson y sus colegas, refiriéndose a la seguridad de los tipos de ataques dañinos que mencionaba en el capítulo 5 como *seguridad,* decían: «La UE es el principal regulador de la privacidad en el mundo, ya que a Washington no le importa y nadie más es lo bastante grande como para preocuparse; debería convertirse también en el principal regulador de la seguridad, o arriesgarse a comprometerse con la misión de seguridad que ya tiene».[22] Si la UE comienza a utilizar su fuerza reguladora de esta manera en materia de seguridad, las empresas lo notarán.

La pregunta es cómo afectará esto al resto del mundo. Hay varias posibilidades.

Los automóviles están diseñados para los mercados locales. Un automóvil que se vende en Estados Unidos es diferente del mismo modelo vendido en México porque las leyes ambientales son diferentes y los fabricantes optimizan los motores para cumplir con las leyes locales; la economía de construir y vender un vehículo permite hacer esta diferenciación con facilidad. En el caso del software es diferente. Es mucho más fácil mantener una versión de un software y venderlo en cualquier lugar, en especial cuando está integrado en un producto. Si las regulaciones europeas imponen estándares de seguridad mínimos en los rúters o en los termostatos conectados a Internet, es probable que se vendan en todo el mundo.[23] (Las leyes sobre emisiones de combustible de California afectan a los coches que se venden en todo Estados Unidos.) Y si las empresas tienen que cumplir con esos estándares de todos modos, es probable que presuman de ello en sus envases.

De la misma manera, esto podría funcionar también con los productos y servicios que ganan dinero con la vigilancia. En abril de 2018, Facebook anunció un cambio en sus prácticas de recopilación de datos, de uso y de retención para los ciudadanos de la UE como resultado del GDPR, pero es poco probable que esos cambios se extiendan a otros países porque no son rentables.[24]

No creo que haya otros mercados lo bastante grandes como para ser de importancia. Singapur cuenta con la Ley de Protección de Datos Personales, Corea del Sur con la Ley de Protección de Información Personal y Hong Kong con la Ordenanza de Datos Personales (Privacidad), pero es difícil saber si son efectivas.[25] Si se aplican, es probable que las compañías afectadas se retiren de esos países en lugar de cambiar sus prácticas comerciales en todo el mundo. Puede haber excepciones para mercados más grandes (y quizá Corea se encuentre en esa categoría) y para dispositivos caros habilitados para Internet, pero puede que no. Soy capaz de imaginar sin ninguna dificultad a los principales fabricantes de automóviles ignorando las regulaciones y desafiando a los Gobiernos a prohibir sus productos y a los gobiernos retrocediendo.

Algunos otros países también están empezando a regular. En 2017, el Tribunal Supremo de la India reconoció el derecho a la privacidad por primera vez en la historia del país,[26] por lo que, al final, esto podría dar como resultado unas leyes más fuertes. Singapur aprobó una nueva Ley de Seguridad Cibernética en 2018, con la que formalizaba estándares mínimos y

obligaciones de informes para proveedores de infraestructura crítica, y estableció un Comisionado de Seguridad Cibernética con amplios poderes de investigación y cumplimiento.[27] Las nuevas regulaciones de seguridad israelíes que afectan a las organizaciones que manejan bases de datos entraron en vigencia en 2018; incluyen requisitos para el cifrado, formación para el personal, pruebas de seguridad y procedimientos de respaldo y recuperación.[28]

Incluso la ONU está empezando a regular. La Comisión Económica para Europa de las Naciones Unidas establece estándares para los automóviles. Sus regulaciones afectan no solo a la UE, sino también a fabricantes de otros países de Europa, África y Asia. Su normativa sin duda afectará a cualquier futuro ordenador autónomo en los vehículos.

En Estados Unidos, algunos estados están tratando de llenar el vacío regulador dejado por el Gobierno federal procesando a compañías con poca seguridad. Nueva York, California y Massachusetts lideran el camino. En 2016, Nueva York multó a los hoteles Trump por filtraciones de datos,[29] y California investigó compañías que hacían un mal uso de los datos de los estudiantes.[30] En 2017, Massachusetts demandó a Equifax[31] y Misuri comenzó a investigar las prácticas de manejo de datos de Google.[32] Treinta y dos fiscales generales del Estado se unieron a la FTC para penalizar al fabricante de ordenadores Lenovo por la instalación de spyware en sus ordenadores portátiles.[33] Incluso la ciudad de San Diego ha demandado a Experian por una filtración de datos en 2013.[34]

En 2017, el Departamento de Servicios Financieros del estado de Nueva York emitió regulaciones de seguridad que afectaban a bancos, aseguradoras y otras compañías de servicios financieros. Las reglas requerían que estas corporaciones tuvieran un director de seguridad de la información, que realizaran pruebas de seguridad periódicas, prestaran formación en concienciación de seguridad a los empleados e implementaran la autenticación de dos factores en sus sistemas. En 2019, estas normas también se aplicarán a sus proveedores y contratistas externos.[35]

En 2017, California presentó temporalmente una ley en la que se exigía a los fabricantes del IoT que divulgaran los datos que recopilaban sobre sus clientes y usuarios,[36] y otros diez estados debatieron la legislación sobre la privacidad del IoT sin que hubiera ningún movimiento federal sobre este tema.[37] Espero más acciones similares en los próximos años.

En enero de 2018, el Senado de California aprobó el proyecto de ley Osos de peluche y tostadoras, que exigía a los fabricantes equipar todos los

dispositivos conectados a Internet que se venden en el estado con las características de seguridad adecuadas a cada uno de ellos.[38] Cuando este libro se imprimió, el proyecto de ley se estaba considerando,[39] al igual que una propuesta para crear una autoridad de protección de datos en California, inspirada por el GDPR.[40]

LO QUE PODEMOS HACER

Así que hemos avanzado algo. Pero, en ausencia de una normativa significativa, ¿qué hacemos?

Podemos intentar comprar comparando los estándares de seguridad, aunque es difícil. Las empresas no hacen públicas sus prácticas de seguridad precisamente porque no quieren que sean un factor que tener en cuenta en las decisiones de compra de los consumidores. Si quieres comprar un DVR con más seguridad porque no quieres que forme parte de una red de robots, no puedes. Si quieres comprar un termostato o un timbre más seguro porque no quieres que nadie te lo piratee, no puedes. Tampoco puedes analizar las prácticas de privacidad y seguridad de Facebook o de Google, solo sus vagas promesas. Hasta que las empresas no utilicen la seguridad y la privacidad como estrategia de diferenciación en el mercado, no podrás basar en ellas tus decisiones de compra. Y si bien una organización como la Unión de Consumidores podría ayudar, solo será parte de una solución más grande.

Hay algunas cosas que los consumidores conscientes sí podemos hacer,[41] como investigar diferentes productos del IoT para intentar determinar cuáles se toman en serio la seguridad y negarnos a comprar aquellos que no lo hacen, ver qué tipos de permisos exige una aplicación para teléfonos inteligentes, tratar de descubrir qué datos se están recopilando y qué se hace con ellos y negarnos a instalar aplicaciones que busquen un acceso irrelevante e invasivo. Admito que esto es mucho pedir y la mayoría de la gente ni se molestará en hacerlo.

En algunos casos podemos decidir no participar, aunque esa opción será cada vez más rara. Así como ahora resulta imposible vivir una vida moderna normal sin una dirección de correo electrónico o una tarjeta de crédito, dentro de poco también lo será no estar conectado al Internet de las cosas. Estas son las herramientas que necesitamos para llevar una vida normal a principios del siglo XXI.

Podemos —y debemos— reforzar nuestra propia ciberseguridad personal. Hay muchos consejos buenos en Internet, la mayoría relacionados con la

privacidad de los datos,[42] pero al final una parte importante de nuestra ciberseguridad no está bajo nuestro control, porque nuestros datos están en manos de otros.

Las empresas tienen más opciones gracias a su tamaño y presupuesto. Por puro interés propio (tanto económico como de reputación), necesitan hacer de la seguridad cibernética una preocupación a nivel directivo. Sí, se trata de riesgos técnicos, pero los ataques ya pueden dañar a una empresa gravemente. Soy director tecnológico de IBM Resilient y asesor especial de seguridad de IBM, y he visto repetidas veces que las decisiones empresariales referentes a la seguridad son más inteligentes cuando la alta dirección está implicada.

Las organizaciones deben conocer la seguridad de los dispositivos y servicios que utilizan tanto en su red como en la nube. Deberán tomar a conciencia cualquier decisión sobre Internet+ y asegurarse de que las nuevas adquisiciones de equipos no afecten involuntariamente a su red. Esta va a ser una ardua batalla. Supongo que las empresas descubrirán que Internet+ se está introduciendo en sus redes de una manera que no esperan ni conocen; alguien comprará una máquina de café o un frigorífico con conexión a Internet, y el sistema de iluminación inteligente, los ascensores o el sistema de control general del edificio se conectarán a la red corporativa interna.

Las empresas necesitan saber dónde están sus datos; puede ser una lucha mantenerlos bajo control en su red. La nube es atractiva: es fácil dejar tus datos en los ordenadores de otras personas sin entender en realidad las repercusiones. Una historia reveladora ocurrida en Suecia salió a la luz en 2017. Dos años antes, la Agencia Sueca de Transporte trasladó todos sus datos a la nube, incluida información clasificada que nunca debería haber abandonado las redes internas del Gobierno.[43] Considero que la persona que tomó la decisión nunca tuvo en cuenta las implicaciones de seguridad.

Las empresas necesitan usar su poder de compra para hacer de Internet+ un lugar más seguro, tanto para ellas como para todos los demás. Deben ejercer presión sobre los fabricantes para mejorar la seguridad, tanto mediante sus propias decisiones de compra como a través de asociaciones de la industria, y deben comprometerse con los legisladores y presionar al Gobierno para que establezca regulaciones para mejorar la seguridad. Aunque las corporaciones son casi patológicamente antirreglamentarias, esta es un área donde una normativa inteligente puede crear nuevos incentivos que de verdad disminuyan el coste general de la seguridad y el de los fallos.

Tenemos que aceptar que estamos atascados con el Gobierno que tenemos, y no con el que desearíamos. Si no podemos confiar en el Gobierno

como el primer promotor de esto, nuestra única esperanza es que las empresas se pongan en marcha y hagan que Internet+ sea seguro de todos modos. No es mucho, pero es lo que tenemos.

Lo que diré sobre la confianza en el capítulo 12 quizá sea lo más importante que debamos recordar. Nos vemos obligados a confiar en todos aquellos cuyos productos y servicios utilizamos. Trata de entender en quién depositas tu confianza y en qué grado, y decide de la manera más inteligente posible. Toma tus decisiones sobre la nube, el Internet de las cosas y todo lo demás con tanto conocimiento y previsión como puedas.

Esto conlleva hacer algunas elecciones difíciles. ¿A quién le permitirás vulnerar tu privacidad y seguridad a cambio de un servicio? ¿Prefieres que acceda a tu correo electrónico Google o Apple? ¿Prefieres regalar tus fotos a Flickr (propiedad de Yahoo) o a Facebook? ¿Prefieres el iMessage de Apple o el WhatsApp de Facebook (o los independientes Signal o Telegram) para tus mensajes de texto?[44]

También significa decidir los países ante los que prefieres ser vulnerable. Las compañías de Estados Unidos están sujetas a las leyes de su territorio y casi con seguridad cederán los datos en respuesta a órdenes judiciales. Almacenar sus datos en otro país puede aislarlas de las leyes estadounidenses, pero estarán sometidas a las de ese otro país. Y aunque la vigilancia global de la Agencia de Seguridad Nacional no tiene parangón en el mundo, la ley de Estados Unidos la limita mucho más de lo que están limitados otros organismos similares en otras partes del mundo —y tus datos están más protegidos legalmente cuando se almacenan en Estados Unidos que cuando se hace en cualquier otro lugar.

Tomar estas decisiones puede ser imposible y, siendo sinceros, la mayoría de las personas no se molestarán en hacerlo. Facebook tiene su sede en California, pero cuenta con centros de datos en todo el mundo, y es probable que tus datos se almacenen en varios de ellos. Muchas empresas con las que tratas utilizan servicios en la nube con datos dispersos por todo el mundo. Sea cual sea el proveedor de servicios con quien decidas tratar, es poco probable que sepas con certeza qué leyes de los países se aplicarán a tus datos, aunque algunas empresas rechazan las solicitudes de datos en función de la ubicación del cliente (como la batalla en curso de Microsoft con el Departamento de Justicia sobre la entrega de datos al FBI de un cliente irlandés almacenados en Irlanda).[45] Veo dos maneras de pensar acerca de esto. La primera es que ya estás sujeto a las leyes de tu país de origen, y lo más prudente es minimizar el número de países adicionales a cuyas leyes estén sujetos tus datos. Por otro

lado, es mucho más probable que te sancionen por cualquier información incriminatoria en tu país de origen, por lo que dificultarle el acceso a la policía sería lo más sensato. Yo elijo la primera opción. En otros lugares he argumentado que, dada la alternativa, preferiría que mis datos estuvieran bajo la jurisdicción del Gobierno de Estados Unidos antes que bajo casi cualquier otro Gobierno del planeta.[46] He recibido muchas críticas por esa opinión, aunque todavía la apoyo.

11

DÓNDE PUEDEN FALLAR LAS POLÍTICAS

EN EL CAPÍTULO ANTERIOR DECÍA que los Gobiernos regulan aquello que mata a la gente. Internet+ está a punto de entrar en esta categoría. Cuando los legisladores se den cuenta de esto, ya no tendremos que elegir entre que haya regulación gubernamental o que no la haya, sino entre una regulación gubernamental inteligente y una estúpida.

Es la estúpida la que me preocupa. Nada estimula tanto a un Gobierno como el miedo; tanto el miedo al ataque como a parecer débil. ¿Recuerdas los meses posteriores a los atentados terroristas del 11 de septiembre? La Ley Patriótica fue aprobada casi por unanimidad y con poco debate, y una Administración republicana de gobierno pequeño creó y financió un organismo gubernamental nuevo que desde entonces ha crecido con rapidez hasta tener casi un cuarto de millón de empleados para proteger la *patria*. No se reflexionó sobre estas acciones y viviremos con las consecuencias los próximos años.

Cualquier cosa que haga el Congreso después de un desastre de seguridad en Internet+ puede ser noticia, pero no es probable que mejore la seguridad. El Congreso podría promulgar leyes y políticas que abordaran de manera inadecuada las amenazas subyacentes, lo que haría que empeorasen los problemas.

Un ejemplo de legislación inadecuada es la Ley de Protección de la Privacidad Infantil en Línea, aprobada en 1998, cuyo propósito era proteger a los menores de la pornografía en Internet. Sus disposiciones no solo eran amplias e inviables, sino que también habrían incorporado una arquitectura de vigilancia generalizada incluso en los rincones más remotos de Internet. Por fortuna, los tribunales impidieron que la ley entrara en vigor.[1] Otra es la DMCA que discutíamos en el capítulo 2; no solo no previene la piratería digital, sino que también perjudica toda nuestra seguridad.[2]

Este capítulo también trata sobre lo que podría suceder a corto plazo y describe algunas de las ideas políticas negativas que se están debatiendo en la

actualidad. Cualquiera de ellas podría convertirse rápidamente en ley después de un desastre.

EXIGIENDO PUERTAS TRASERAS

En el capítulo 9 hablaba de la necesidad de anteponer la seguridad a la vigilancia y de cómo los Gobiernos a menudo trabajan en contra de este principio. La NSA lo hace a escondidas debilitando el cifrado. El FBI quiere hacerlo públicamente forzando a las compañías a incluir puertas traseras en sus sistemas de cifrado.

Esta exigencia no es nueva. Casi siempre desde 1990, las fuerzas del orden de Estados Unidos han afirmado que el cifrado se ha convertido en una barrera insuperable para la investigación criminal. En la década de 1990 surgió la alarma sobre las llamadas telefónicas encriptadas. En el año 2000, los representantes del FBI, en sus discusiones sobre el cifrado, comenzaron a referirse a los peligros de *oscurecer* y cambiaron su preocupación a las aplicaciones de mensajería cifrada. En la década de 2010, los teléfonos inteligentes cifrados se han convertido en el nuevo peligro.

La retórica es uniformemente grave.

Así hablaba el director del FBI Louis Freeh, quien asustó al Comité de Inteligencia Permanente de la Cámara de Representantes en 1997: «El uso generalizado de un cifrado sólido e irrompible en última instancia devastará nuestra capacidad para combatir el crimen y prevenir el terrorismo».[3]

Por su parte, la consejera general del FBI Valerie Caproni asustó al Comité Judicial de la Cámara de Representantes en 2011: «Cuanto más grande es la brecha entre el poder y las competencias, más incapaz es el Gobierno de recoger pruebas valiosas en casos que van desde la explotación infantil y la pornografía hasta el crimen organizado y el tráfico de drogas, pasando por el terrorismo y el espionaje: pruebas que un tribunal ha autorizado al Gobierno a recoger. Esta brecha representa una amenaza creciente para la seguridad pública».[4]

El director del FBI James Comey, por otro lado, asustaba al comité judicial del Senado en 2015 de la siguiente manera: «Es posible que no podamos identificar y detener a los terroristas que utilizan las redes sociales para reclutar, planificar y ejecutar un ataque en nuestro país. Es posible que no podamos erradicar a los depredadores de niños que se esconden en las sombras de Internet, o encontrar y arrestar a criminales violentos que se dirigen a nuestros vecindarios. Es posible que no podamos recuperar

información crítica de un dispositivo que pertenece a una víctima que no nos puede proporcionar la contraseña, sobre todo cuando el tiempo es clave».[5]

Y aquí está el fiscal general adjunto Rod Rosenstein tratando de asustarme a mí (yo estaba en la audiencia de la Cumbre Cibernética de Cambridge en 2017):

> «Pero la llegada del cifrado "a prueba de órdenes judiciales" es un grave problema. Amenaza con desestabilizar el equilibrio constitucional entre privacidad y seguridad que existe desde hace más de dos siglos. Nuestra sociedad nunca ha tenido un sistema en el que la evidencia de irregularidades criminales fuera totalmente inmune a la detección, incluso cuando la policía obtiene una orden judicial autorizada. Pero ese es el mundo que las empresas de tecnología están creando».[6]

Los cuatro jinetes del apocalipsis de Internet (terroristas, narcotraficantes, pedófilos y crimen organizado) siempre asustan a la gente. «A prueba de órdenes judiciales» es una frase bastante aterradora, pero solo significa que una de esas órdenes no obtendrá la información. Los papeles quemados en una chimenea también son *a prueba de órdenes*.

La noción de que el mundo nunca ha visto una tecnología inmune a la detección es absurda. Antes de Internet, muchas comunicaciones nunca estaban disponibles para el FBI; cada conversación de voz desaparecía irrevocablemente tras pronunciar las palabras. Nadie, sin contar a las autoridades, podría retroceder en el tiempo y recuperar una conversación o seguir los movimientos de alguien. Dos personas podrían salir a caminar en un área aislada, mirar a su alrededor y no ver a nadie, y confiar en una privacidad que ahora se ha perdido para siempre. Hoy vivimos en la edad de oro de la vigilancia.[7] Como decía en el capítulo 9, lo que necesita el FBI son conocimientos técnicos, no puertas traseras.

A lo largo de las décadas, el Gobierno ha propuesto una variedad de puertas traseras. En los noventa, el FBI sugirió que los desarrolladores de software proporcionaran copias de cada clave de cifrado. La idea se denominó *depósito de claves*, similar a todos los que tienen que entregarle a la policía una copia de la llave de su casa.[8] A principios de 2000, el FBI argumentó que los proveedores de software deberían insertar deliberadamente vulnerabilidades en los sistemas informáticos para que fueran explotadas por la policía cuando fuera necesario.[9] Una década más tarde las demandas se convirtieron en un método más general para *averiguar cómo hacer esto*.[10]

Hace poco, el FBI sugirió que las empresas tecnológicas utilizaran su proceso de actualización para enviar actualizaciones falsas a usuarios específicos e instalar puertas traseras en paquetes de software individuales por encargo. Rosenstein le ha dado a esta propuesta hostil de seguridad el nombre amigable de *encriptación responsable*.[11] Para cuando leas esto podría haber una solución preferida diferente.

Esto no ocurre solo en Estados Unidos. Los legisladores de Reino Unido ya están insinuando que la Ley de Poderes de Investigación de 2016 les otorga el poder de obligar a las empresas a sabotear su propio cifrado.[12] En 2016, Croacia, Francia, Alemania, Hungría, Italia, Letonia y Polonia instaron a la UE a que exigiera que las empresas agregaran puertas traseras.[13] (Por separado, la UE está considerando una legislación que prohíbe las puertas traseras.)[14] Australia también está tratando de exigir el acceso.[15] En Brasil, los tribunales cerraron temporalmente WhatsApp tres veces en 2016 porque la policía local no pudo acceder a los mensajes cifrados.[16] Egipto bloqueó la aplicación de mensajería cifrada Signal.[17] Muchos países prohibieron los dispositivos BlackBerry hasta que la empresa permitió a los Gobiernos escuchar las comunicaciones. Y tanto Rusia[18] como China[19] bloquean de manera habitual aplicaciones que no pueden controlar.

No importa cómo se llamen o cómo se hagan, incorporar puertas traseras para la aplicación de la ley en ordenadores y sistemas de comunicaciones es una idea terrible. Va contra nuestra necesidad de primar la seguridad sobre la vigilancia. Si bien en teoría sería fantástico que la policía pudiera espiar a sospechosos, reunir pruebas forenses o investigar de otro modo los delitos (suponiendo que existieran las políticas y las garantías adecuadas), no hay forma de diseñar esto de forma segura. Es imposible construir un mecanismo de puertas traseras que solo funcione en presencia de una orden judicial o cuando un agente de la ley trate de usarlo con fines legítimos. O la puerta trasera funciona para todos o para nadie.

Esto significa que cualquier puerta trasera hará que todos estemos menos seguros. La utilizarán Gobiernos y delincuentes extranjeros contra nuestros líderes políticos, nuestra infraestructura crítica, nuestras empresas…, contra todo. Se utilizará contra nuestros diplomáticos y espías en el extranjero y contra nuestros agentes del orden en casa. Se utilizará para cometer delitos, facilitar el espionaje del Gobierno y habilitar los ataques cibernéticos. Es una idea increíblemente estúpida.

Si Estados Unidos impone con éxito los requisitos de puertas traseras a las empresas estadounidenses, no hay nada que impida que otros Gobiernos

hagan lo mismo. Todo tipo de países represivos, desde Rusia y China hasta Kazajistán y Arabia Saudí, exigirán el mismo nivel de *acceso legal*, a pesar de que sus leyes están diseñadas para castigar a los disidentes políticos.

La idea de Rosenstein de utilizar el proceso de actualización es particularmente perjudicial; ya hay vulnerabilidades en él. Todos estamos más seguros cuando instalamos actualizaciones lo más rápido posible. Una medida de seguridad que estamos empezando a ver es una mayor transparencia, por lo que los sistemas individuales pueden estar seguros de que la actualización que están recibiendo está autorizada por la empresa y se aplica a todos los usuarios. Esto es importante para la seguridad; recuerda el capítulo 5 cuando hablaba sobre los atacantes que interfieren en el proceso de actualización para distribuir malware. Los requerimientos del FBI evitarían que las compañías fueran transparentes e incluyeran otras medidas de seguridad en el proceso de actualización.

Si el mecanismo de actualización es un método conocido por la policía para piratear los ordenadores y los dispositivos de alguien, mucha gente desactivará la actualización automática. Esta pérdida de confianza tardará años en recuperarse y el efecto general sobre la seguridad será devastador. Sería como esconder tropas de combate en vehículos de la Cruz Roja; no lo hacemos, aunque sea una táctica efectiva.

A fin de cuentas, usar el proceso de actualización para permitir la distribución de malware lo haría mucho menos seguro. Si una actualización tiene lugar con poca frecuencia, una empresa puede crear una seguridad sólida en torno al proceso de autenticación. Si una empresa como Apple recibe múltiples solicitudes al día para desbloquear teléfonos (el FBI afirmó en 2017 que tenía siete mil teléfonos que no pudo desbloquear),[20] los procedimientos de rutina que tendría que implementar para responder a esas solicitudes serían mucho más vulnerables a los ataques.

Quienes entienden de seguridad saben que las puertas traseras son peligrosas. Un grupo de trabajo del Congreso de 2016 concluyó que «cualquier medida que debilite el cifrado funciona contra el interés nacional».[21] Lord John Evans, quien dirigía el MI5 del Reino Unido, dijo lo siguiente: «Mi opinión personal es que no debemos socavar la fuerza de la criptografía en todo el conjunto del mercado cibernético porque creo que el coste de hacerlo sería considerable».[22]

Lo más importante de todo: darle al FBI lo que quiere no resolverá este problema.

Incluso aunque el FBI logre obligar a las grandes empresas estadounidenses —como Apple, Google y Facebook— a hacer inseguros sus dispositivos y sistemas de comunicaciones, muchos otros competidores más pequeños ofrecerán productos seguros. Si Facebook instala una puerta trasera en WhatsApp, los tipos malos se moverán a Signal. Si Apple incluye una puerta trasera en su cifrado de iPhone, los malos se trasladarán a una de las otras muchas aplicaciones cifradas de voz.[23]

Incluso el FBI es menos exigente en privado. Según las conversaciones que otros y yo hemos tenido con funcionarios del FBI, por lo general están de acuerdo con el cifrado opcional, ya que la mayoría de los malos no se molestan en activarlo. A lo que se oponen es al cifrado por defecto.

Y esa es precisamente la razón por la que lo necesitamos. Los valores predeterminados son poderosos: la mayoría de nosotros o no sabemos lo suficiente, o no nos molestamos en activar las funciones de seguridad opcionales en nuestros ordenadores, teléfonos, servicios web, dispositivos IoT y todo lo demás. Y si bien el FBI tiene razón en que el delincuente promedio no activará el cifrado opcional, sí cometerá otros errores que lo harán susceptible de ser investigado (sobre todo si el FBI mejora sus técnicas de investigación digital). Es el criminal inteligente el que debería preocupar al FBI, y esos criminales usarán las alternativas más seguras.

Las puertas traseras dañan al usuario promedio de Internet, a los buenos y a los malos, aunque el FBI se enfoca de forma miope y exagerada en los malos. No obstante, una vez que nos damos cuenta de que hay muchos más chicos buenos en Internet que malos, es obvio que los beneficios de un cifrado fuerte en todas partes compensan las desventajas de darles también a los delincuentes acceso a este tipo de cifrado.

LIMITANDO EL CIFRADO

En Estados Unidos, antes de mediados de la década de 1990, la encriptación estaba regulada como una munición. Los productos de software y hardware que utilizan cifrado estaban controlados por la exportación, igual que las granadas o los rifles. El cifrado fuerte no podía exportarse, y cualquier producto para la exportación tenía que ser lo bastante débil para que la NSA pudiera entrar en él de forma sencilla. Estos controles terminaron cuando Internet y la comunidad tecnológica internacional los volvieron obsoletos porque la noción de *exportación* de software ya no tenía sentido.[24]

Se habla de volver a los controles de cifrado. En 2015, el entonces primer ministro británico David Cameron propuso prohibir por completo el cifrado fuerte en su país[25] y la actual primera ministra Theresa May se hizo eco de esto después del ataque terrorista del puente de Londres en 2017.[26]

Esto sería dar un paso más allá de las puertas traseras obligatorias en los sistemas de encriptación populares, como WhatsApp y iPhone, y supondría que cualquier sistema informático, software o servicio con cifrado fuerte fuera ilegal. El problema, por supuesto, es que las leyes de un país son nacionales, mientras que el software es internacional. En 2016, examiné el mercado de productos de encriptación;[27] de los 865 productos de software de 55 países diferentes, 811 eran inmunes a una prohibición en el Reino Unido porque fueron creados fuera del país. Si Estados Unidos aprobara una prohibición similar, 546 productos serían inmunes.

Mantener esos productos extranjeros fuera de un país sería imposible;[28] requeriría impedir que los motores de búsqueda encontraran productos de encriptación extranjeros; controlar todas las comunicaciones para garantizar que nadie descargara un producto de cifrado extranjero desde un sitio web; inspeccionar cada ordenador, teléfono y dispositivo del IoT que entre en el país, ya sea transportado por una persona a través de la frontera o enviado por correo; prohibir el software de código abierto y los repositorios de código en línea, y prohibir e interceptar en la frontera libros que contengan algoritmos y códigos de cifrado. En resumen, una auténtica locura.

Si se intentara, el resultado de tal prohibición sería incluso peor que exigir puertas traseras. Nos obligaría a todos a estar mucho menos seguros ante cualquier amenaza, situaría a las empresas nacionales que tuvieran que cumplir con esto en una desventaja competitiva frente a las que no y les daría a los criminales y a los Gobiernos extranjeros una enorme ventaja.

No veo probable que esto suceda, pero es factible. En el último año he visto un cambio en la retórica en torno a la encriptación. En sus intentos por conseguir puertas traseras, los funcionarios del Departamento de Justicia se apresuran a pintar el cifrado como una herramienta criminal con referencias evocadoras a los cuatro jinetes del apocalipsis de Internet y a servicios de anonimato como Tor.[29] En un frente diferente por completo, *cripto* está comenzando a usarse como una abreviatura de *criptomonedas*, como bitcóin, y se propone como una herramienta para aquellos que quieren comprar productos ilegales en la aterradora red oscura. El resultado es que los usos positivos de la criptografía y su forma de proteger toda nuestra seguridad se

están eliminando de la conversación. Si esta tendencia continúa, veremos propuestas serias que quieren prohibir el cifrado fuerte.

En 2015, Mike McConnell, Michael Chertoff y William Lynn, antiguos altos funcionarios gubernamentales con amplia experiencia en estos asuntos, escribieron sobre la importancia de la seguridad de los ordenadores y de Internet para la seguridad nacional:

> Creemos que el mayor bien común es una infraestructura de comunicaciones segura protegida por encriptación ubicua a nivel de dispositivos, servidores y empresas que no incluyan medios para el control gubernamental.[30]

Estos sentimientos son contrarios a la postura oficial de sus antiguos empleadores, pero se retiraron sin incidentes y como figuras muy respetadas, así que los tres se sintieron con libertad para hablar. Necesitamos cambiar la postura oficial del Gobierno para que todos trabajen por una mayor seguridad para todos.

PROHIBIENDO EL ANONIMATO

Se pide con frecuencia la prohibición del anonimato en Internet. Estas peticiones provienen de quienes quieren controlar el discurso de odio y acoso bajo el supuesto de que, si saben quiénes son los troles, pueden desterrarlos o, mejor aún, estos se avergonzarían de comportarse así; provienen de aquellos que quieren prevenir el ciberdelito al suponer que ser capaces de identificar a alguien nos hace más fácil detenerlo; provienen de quienes quieren arrestar a los spammers, a los acosadores, a los traficantes de drogas y a los terroristas.

La prohibición del anonimato adopta varias formas, pero básicamente puedes pensar en ello como si nos dieran a todos el equivalente en Internet de un permiso de conducir. Todos usaríamos ese permiso para configurar nuestros ordenadores y registrarnos en varios servicios, como las cuentas de correo electrónico, y nadie tendría acceso sin uno.

Esto no funcionará por cuatro razones.

Primero, no tenemos una infraestructura en el mundo real para proporcionar credenciales de usuario de Internet basadas en otros sistemas de identificación: pasaportes, documentos de identidad nacionales, permisos de conducir, o lo que sea. Recuerda lo que decía en el capítulo 3 sobre la identificación y los documentos de filiación e identidad. Segundo, un sistema

como este podría hacer que el robo de identidades fuera más excepcional, aunque también mucho más rentable.

Estas dos razones explican por qué la identificación obligatoria para el uso de Internet es una mala idea. En este momento hay un montón de sistemas adecuados de identificación y de autenticación. Los bancos se administran lo bastante bien como para dejarte transferir dinero en línea, y las empresas como Google y Facebook se administran a la perfección como para permitirles a otros utilizar sus sistemas. Hay varias aplicaciones de pago de teléfonos inteligentes que compiten. Tu número de teléfono móvil se está convirtiendo en un identificador único con fines como la autenticación de dos factores.

Sin embargo, cuando construimos un sistema de identificación obligatorio, necesitamos alcanzar justo a aquellas personas que desean sabotear el sistema. Todos los sistemas de identificación existentes ya han sido saboteados por adolescentes intentando comprar alcohol en transacciones cara a cara. Instaurar un sistema de identificación obligatorio en Internet sería mucho más difícil.

En tercer lugar, cualquier sistema de este tipo tendría que funcionar de forma global. Pero ten en cuenta que cualquier persona del país que sea puede fingir ser de otro lugar. Si Estados Unidos prohibiera el anonimato y ordenara a sus ciudadanos que usaran su permiso de conducir para registrarse personalmente en una dirección de correo electrónico, cualquier estadounidense podría tener una cuenta de correo electrónico anónima de un país sin requisitos de identificación. Entonces, o bien reconocemos que cualquier persona puede conseguir una dirección de correo electrónico anónima, o bien prohibimos la comunicación con el resto del mundo. Ninguna de las opciones va a funcionar.

Cuarto, y más importante, siempre es posible configurar un sistema de comunicación anónimo sobre uno identificado. Tor es un sistema de navegación web anónima utilizado tanto por disidentes políticos como por delincuentes de todo el mundo. No voy a decir cómo funciona aquí, pero puede proporcionar anonimato incluso aunque todos en el sistema estén identificados.

Estas son las razones por las que prohibir el anonimato no funciona. Es terrible porque es malo para la sociedad. El discurso anónimo es valioso,[31] y en algunos países salva vidas. La capacidad de un individuo de ejercer múltiples roles en cada aspecto de su vida es valiosa. Prohibir el anonimato

sacrificaría una libertad esencial a cambio de una ilusión de seguridad temporal.

Esto no significa que todos merezcamos el anonimato para todas las cosas; la sociedad ya lo prohíbe en muchas áreas. No te permiten conducir un automóvil anónimo en vías públicas: todos los coches deben llevar matrícula; reglas similares están próximas para los drones. Estados Unidos les ha impuesto a los bancos de todo el mundo normas de conocimiento de sus clientes. El límite entre los espacios donde se permite el anonimato y donde está prohibido parece ser el punto donde alguien podría causar un daño físico o económico significativo. A medida que Internet+ cruce ese límite, cuenta con que haya más espacios con menor anonimato.

PRACTICANDO LA VIGILANCIA MASIVA

La vigilancia masiva no se limita a los países totalitarios. El Gobierno de Estados Unidos recopiló los metadatos de las llamadas telefónicas de la mayoría de los estadounidenses hasta 2015 y aún tiene acceso a esta información.[32] (Los metadatos consisten en detalles sobre quién llama a quién, cuándo y durante cuánto tiempo, pero no el contenido de las conversaciones.) Muchos Gobiernos locales conservan la información completa sobre los movimientos de las personas recopilados por escáneres de matrículas montados en postes de calles y en furgones móviles.[33] Y, por supuesto, muchos organismos nos tienen a todos bajo vigilancia a través de una variedad de mecanismos. Los Gobiernos exigen con regularidad acceso a esos datos de manera que no requieran una orden judicial: citaciones y cartas de seguridad nacional.[34]

Me preocupa que algunos de los riesgos catastróficos sobre los que escribía en el capítulo 5 lleven a los legisladores a ir más allá de las puertas traseras y de la criptografía debilitada para autorizar una vigilancia doméstica ubicua. Dejando de lado los efectos de *1984*, que hacen que sea una idea terrible a primera vista, la efectividad de la vigilancia ubicua es muy limitada; solo es útil entre el momento en que es posible una nueva capacidad y el momento en que se vuelve fácil.

Para comprender cómo podría suceder esto, ten en cuenta en particular la curva de desarrollo de cualquier tecnología destructiva. En los primeros días del desarrollo, los escenarios superdañinos no son posibles. En la actualidad, por ejemplo, a pesar de lo que la televisión y las películas reflejen, no

tenemos los conocimientos técnicos necesarios para crear un supergermen que pueda matar a millones de personas.

Conforme se desarrolla la ciencia biológica, los escenarios catastróficos se hacen posibles, pero son muy costosos. Convertirlos en realidad requeriría un esfuerzo organizado de una magnitud similar a la del Proyecto Manhattan de la Segunda Guerra Mundial o esfuerzos militares similares para desarrollar y construir armas biológicas.[35]

A medida que la tecnología continúa mejorando, las capacidades dañinas se vuelven más baratas y están disponibles para grupos cada vez más pequeños y menos organizados. Es probable que en algún momento una conspiración cause una catástrofe. Para ello se requeriría dinero y experiencia, pero tanto lo uno como lo otro pueden adquirirse. Uno podría pensar en un esfuerzo a gran escala para perturbar la economía mundial mediante ataques coordinados a los sistemas informáticos de la bolsa de valores o a la infraestructura crítica, como las centrales eléctricas o los sistemas de navegación de las aerolíneas.

Este es el punto en el que la vigilancia ubicua puede ofrecernos seguridad. La esperanza estaría en detectar la conspiración en sus etapas de planificación y recopilar pruebas suficientes para conectar los puntos e interrumpir el complot antes de que suceda. Esta es la principal justificación de los actuales esfuerzos de vigilancia ubicuos de la NSA contra el terrorismo.

Pero, aunque la vigilancia ubicua podría tener éxito en la mayoría de estos casos, en especial contra atacantes menos expertos técnicamente, fallaría contra los atacantes más motivados, más capacitados y mejor financiados. Mientras que la tecnología mejora, el número de conspiradores y la cantidad de planificación requerida para desatar el caos se reducen aún más haciendo que la detección basada en la vigilancia sea aún menos efectiva. Piensa en la bomba de fertilizantes de Timothy McVeigh y en los cómplices que lo ayudaron a atacar el edificio federal Alfred P. Murrah. Tal vez la vigilancia ubicua pudiera haber detectado la conspiración en las etapas de planificación y compra, pero quizá no. La vigilancia focalizada, basada en el anticuado trabajo policial de seguimiento de pistas, podría identificar de manera más efectiva a quienes defienden el derrocamiento violento del Gobierno de Estados Unidos y se dedican a ensamblar materiales para fabricar bombas.

Cuanto más mejora la tecnología y tan solo una o dos personas pueden causar una catástrofe, la vigilancia ubicua se vuelve inútil. Ya conocemos incidentes como este. Ningún tipo de vigilancia puede detener los tiroteos en masa como los de Fort Hood (2009), San Bernardino (2015) o Las Vegas

(2017).[36] Ninguna vigilancia pudo haber detenido los ataques DDoS contra Dyn. El hecho de no anticipar el atentado de la maratón de Boston no fue un fallo en la vigilancia masiva, sino en el seguimiento de las pistas de investigación, si es que puede considerarse un fracaso.[37]

En el mejor de los casos, la vigilancia masiva solo puede servirle a la sociedad para ganar tiempo. Aun así, no serviría para mucho. La vigilancia es más efectiva para el control social que para prevenir delitos, por ello es una herramienta tan popular entre los Gobiernos autoritarios.

Esto no significa que no vayamos a ser testigos de una vigilancia masiva doméstica, en especial después de otro ataque terrorista catastrófico. Por muy mal que nos estemos defendiendo contra lo que percibimos como peligros catastróficos, somos muy buenos sintiendo pánico en situaciones específicas relacionadas con amenazas. E históricamente el pánico es mucho más peligroso para la libertad que el peligro real en sí mismo. Además, siempre habrá nuevas amenazas tecnológicas en diferentes puntos a lo largo de la curva de desarrollo, cada una de las cuales justificará la vigilancia masiva.

CONTRAATACANDO

Hackear a quien nos hackea es otra idea terrible, aunque con frecuencia asoma su fea cabeza. En esencia, es un contraataque privado. Es una organización que se lanza a la ofensiva para tomar represalias contra sus atacantes. A veces pasa por el eufemismo de *defensa cibernética activa*,[38] pero ese nombre solo sirve para ocultar lo que es en realidad: un combate de servidor contra servidor. Hoy es ilegal en todos los países, pero se habla constantemente de hacerlo legal.

A sus defensores les gusta mencionar dos escenarios específicos que podrían justificar la piratería: el primero se refiere a cuando las víctimas conocen la ubicación de sus datos robados: podrían piratear el ordenador y borrarlos; el segundo escenario hacer referencia a cuando existe un ataque en curso: podrían piratear el ordenador del atacante y detenerlo al momento.

En apariencia esto parece razonable, aunque también podría convertirse en un desastre muy deprisa.[39] Primero, están las dificultades de atribución de las que hablaba en el capítulo 3. ¿Cómo puede una organización estar segura de quién la ataca, y qué ocurre si penetra por error en una red inocente para tomar represalias? Es fácil disfrazar la fuente de un ataque o dirigirlo a través de un intermediario.

Segundo, ¿qué sucede si un *hackbacker* (un hacker que toma represalias contra otro hacker) penetra en una red de un país extranjero? O, peor, el ejército de ese país. Es casi seguro que se consideraría un delito y podría causar un incidente internacional. Muchos países utilizan sustitutos, compañías de primera línea y criminales para hacer el trabajo sucio en Internet, por lo que las posibilidades de un fallo, un error de cálculo o una mala interpretación son altas. La autorización de hackear como represalia aumentaría el desorden, y no queremos que ninguna compañía inicie una guerra cibernética por accidente.

Tercero, la piratería está lista para el abuso. Cualquier organización podría ir contra un competidor atacando a sus propios servidores o instalando archivos confidenciales en la red de su competidor y luego pirateándolos.

Cuarto, sería fácil que las hostilidades fueran en aumento. Un emprendedor podría conspirar iniciando una batalla entre dos organizaciones simulando pirateos entre ellas.

En quinto y último lugar, no está claro si esta es siquiera una táctica efectiva. La venganza es satisfactoria, pero no hay evidencia de que este tipo de pirateo mejore la seguridad o tenga un efecto disuasorio.[40]

Sin embargo, la verdadera razón por la que esta es una idea terrible es que permite que la gente se tome la ley por su cuenta. Existen razones por las cuales no se te permite entrar en casa de tu vecino para recuperar un artículo, incluso aunque sepas que te lo ha robado. Hay un motivo por el que ya no emitimos patentes de corso, esas mismas que autorizaron a los buques mercantes privados a atacar y capturar otros barcos. Este tipo de capacidades son, con razón, de uso exclusivo de los Gobiernos.

Casi todo el mundo está de acuerdo con esto.[41] Tanto el FBI como el Departamento de Justicia advierten contra la piratería por venganza.[42] Un proyecto de ley de 2017 que legitimaba algunas tácticas de hackeo como represalia murió al tener un apoyo mínimo.[43] La principal excepción parece ser Stewart Baker (abogado y antiguo funcionario sénior de la NSA y del DHS), quien regularmente recomienda hackear como represalia.[44] También algunas empresas de ciberseguridad de todo el mundo están presionando para obtener autorización legal para ofrecer servicios de hackeo por venganza a clientes corporativos. Israel parece querer ser el país base para esta industria.

A pesar de su ilegalidad, el hackeo por venganza ya está ocurriendo. Las compañías que ofrecen servicios de este tipo no se anuncian abiertamente y es probable que las contraten mediante compañías intermediarias y con contratos

negables. Igual que el soborno corporativo, es algo que existe, y algunas empresas violan el derecho internacional al participar en esta práctica.

Supongo que siempre será así. Con independencia de lo que haga Estados Unidos y los países con ideas afines, otros serán refugios seguros para esta práctica. Esto significa que debemos tratar la piratería como un soborno: tenemos que declararla ilegal en todo el mundo y procesar a las empresas estadounidenses que participen en ella. Tenemos que presionar para conseguir tratados y normas internacionales contra la piratería por represalia y esforzarnos al máximo por marginar las anomalías. En este momento no hay una postura oficial de Estados Unidos respecto a la piratería, aunque creo que pronto la habrá.

RESTRINGIENDO LA DISPONIBILIDAD DE SOFTWARE

Históricamente, a menudo nos hemos basado en la escasez para acercarnos a la seguridad. Es decir, nos protegemos de los usos maliciosos de algo al hacer que sea difícil de obtener. Esto ha funcionado bien para algunas cosas (me vienen a la mente el polonio-210, el virus de la viruela o los misiles antitanques) y menos para otras: el alcohol, las drogas, las pistolas. Internet+ destruye ese modelo.

El espectro radioeléctrico está muy regulado, y existen numerosas normas sobre quién puede transmitir y en qué frecuencias; algunas están reservadas para los militares, otras para la policía y otras para las comunicaciones entre las aeronaves y el control en tierra. Hay frecuencias en las que solo puedes transmitir si tienes una licencia, y otras en las que solo puedes transmitir si cuentas con un dispositivo de comunicaciones específico.

Antes de los ordenadores, todo esto se hacía cumplir limitando los tipos de radios disponibles para la venta. Una radio normal solo sintonizaría las frecuencias legales. Esta solución no era perfecta: siempre era posible comprar o construir una radio que pudiera transmitir o recibir en otros canales, aunque era una solución complicada que requería conocimientos especializados (o al menos acceso a equipos especializados); no era una solución de seguridad perfecta, pero sí lo bastante buena para la mayoría de los propósitos. Hoy en día, las radios son solo ordenadores con antenas conectadas, y puedes comprar una tarjeta de radio definida por software para tu PC que te permitirá transmitir en cualquier frecuencia.

En el capítulo 4 hablaba sobre los riesgos de las personas que piratean sus propios ordenadores para evadir leyes que son razonables, sobre la posibilidad

de que las personas modifiquen el software de su automóvil para violar las leyes de control de emisiones, sus impresoras 3D para fabricar objetos que infringen leyes de derechos de autor o las impresoras biológicas que van contra las leyes sobre matar a un gran número de personas.

Para cada una de estas nuevas tecnologías, tendremos llamadas de atención perfectamente razonables que intenten restringir lo que los usuarios pueden hacer con sus dispositivos. Por ejemplo, lo que Mattel, Disney, los censores y los defensores del control de armas van a querer es una impresora 3D que le permita al cliente fabricar cualquier cosa, excepto aquello que esté en una lista de objetos prohibidos.[45]

Esto es justo lo mismo que el problema con los derechos de autor. La gestión de derechos digitales era una solución técnica que falló, y la DMCA fue la ley que vino después. Solo ha sido eficaz para evitar que los aficionados hagan copias de música y películas digitales, pero no ha impedido que los profesionales hagan lo mismo ni la difusión de trabajos con derechos de autor con las protecciones DRM eliminadas.

El temor a un software pirata en los vehículos autónomos o la impresión de virus asesinos será mucho mayor que el miedo a las canciones copiadas ilegalmente. Las industrias que se verán afectadas son mucho más poderosas que la del entretenimiento. Tanto el Gobierno como el sector privado analizarán la experiencia de la industria del entretenimiento con DRM y concluirán que el problema es que los ordenadores son, por naturaleza, extensibles. Se fijarán en la DMCA y concluirán que la ley no fue lo bastante onerosa y restrictiva. Me preocupa que las leyes análogas para impresoras 3D, bioimpresoras, automóviles, etc., sean respaldadas por intereses gubernamentales y privados que trabajen juntos contra los usuarios.[46]

Las leyes que restringen el acceso al software que les permite a las personas modificar sus ordenadores IoT pueden ir en contra de la mayoría de la gente durante un tiempo, pero al final serían ineficaces, porque Internet permite el libre flujo de software e información en todo el mundo, y porque unas leyes así nunca mantendrían a los ordenadores fuera de un país. Esto no es solo una cuestión de aceptar la solución más efectiva y vivir con las excepciones. Cuando se trata de canciones y otro contenido digital, el coste del fracaso es mínimo; con estas nuevas tecnologías, el coste del fracaso será mucho mayor.

Necesitamos resolver estos problemas de inmediato. No con leyes que limiten el uso de la tecnología o de las capacidades del ordenador, sino desarrollando capacidades compensadoras.

Con respecto a las radios, una solución sería permitir que todas se vigilen a sí mismas.[47] Las radios podrían transformarse en una red de detección que ubique transmisores malintencionados o mal configurados y luego envíe esa información a la policía, quien podría investigar las presuntas infracciones. Los sistemas de radio podrían estar diseñados para resistir los intentos de escuchas y de atascos para que los transmisores no autorizados no puedan interferir con su funcionamiento. Por supuesto, habría detalles que concretar. Mi objetivo aquí no es resolver el problema técnico, solo demostrar que se pueden encontrar soluciones.

Esta es una lección general que se aplicará a muchos aspectos de Internet+, desde el 3D y las bioimpresoras hasta algoritmos autónomos e inteligencia artificial. Si vamos a vivir en un mundo donde las personas puedan causar daños generalizados, al final tendremos que descubrir cómo zafarnos de las amenazas inherentes a cada sistema. Las restricciones de tipo DMCA nos darán un poco de tiempo, pero no resolverán nuestros problemas de seguridad.

12

HACIA UN INTERNET FIABLE, RESILIENTE Y PACÍFICO

LOS SERES HUMANOS NOS BASAMOS en la confianza. Ninguna otra especie confía ni remotamente de la forma en que nosotros lo hacemos. La sociedad fracasaría sin confianza; de hecho, nunca habría llegado a constituirse sin ella. Confiamos todo el tiempo, a lo largo de nuestros días, sin siquiera pensarlo dos veces. Y no es que tengamos otra opción. Confiamos en que la comida de nuestros supermercados no nos enferme, en que las personas con las que nos topamos por la calle no nos ataquen, en que los bancos no roben nuestro dinero o en que los otros conductores no choquen contra nosotros. Por supuesto, mientras lees esto estás pensando en advertencias y en excepciones, pero la razón por la que estás pensando en ellas es porque son muy raras. A menos que estés viviendo en una parte del planeta sin ley, todos los días confías a ciegas en millones de personas, en organizaciones e instituciones. El hecho de que apenas lo pensemos es una prueba de lo bien que funciona el sistema.

Piensa en tu ordenador y en todas las compañías en las que estás obligado a confiar solo por usarlo. Confías en los diseñadores, en los fabricantes de los chips que hay en su interior y en la empresa que los ensambla; de hecho, confías en toda la cadena de suministro, desde el fabricante hasta la empresa que te lo vendió. Confías en la compañía que escribió su sistema operativo, probablemente Microsoft o Apple, y en las que escribieron el software que estás usando —esto incluye aplicaciones como tu navegador y procesador de textos— y en el software de seguridad, como el programa antivirus que usas. Confías en los servicios de Internet que estás utilizando: en tu proveedor de correo electrónico, en tus plataformas de redes sociales y en cualquier servicio en la nube que maneje tus datos. Confías en tu proveedor de servicios de Internet y en las compañías que diseñaron, construyeron e instalaron el rúter de tu hogar. Seguro que hay docenas de empresas en las que no tienes más remedio que confiar, junto con los Gobiernos de los países a los que

pertenecen. Cualquiera de ellas tiene la capacidad de subvertir tu seguridad y de aprovecharse de ti, y esa falta de seguridad en los procesos facilita que otros hagan lo mismo.

Confías en todas estas entidades porque tienes que hacerlo, no porque creas que alguna de ellas es fiable. En Internet, el universo de actores fiables se está reduciendo de manera considerable.[1] Una encuesta de 2017 demostró que el 70 % de los estadounidenses cree que es al menos probable que el Gobierno esté supervisando sus llamadas telefónicas y sus correos electrónicos.[2] La gente de todo el mundo desconfía de la NSA y de Estados Unidos en general.

El informe de ciberseguridad de Obama de 2016 del que hablaba en el capítulo 10 lo manifestaba de esta manera:

> El éxito de la economía digital depende en última instancia de individuos y de organizaciones que confían en la tecnología informática y que confían en las organizaciones que proporcionan productos y servicios que recopilan y retienen datos. Esa confianza es menos sólida de lo que era hace algunos años debido a los incidentes y las infracciones exitosas que han generado temores de que los datos corporativos y personales se vean comprometidos y sean mal utilizados. También ha aumentado la preocupación por la capacidad de los sistemas de información para evitar que se manipulen los datos: las elecciones de 2016 en Estados Unidos aumentaron la conciencia pública sobre este tema. En la mayoría de los casos, la manipulación de datos es una amenaza más peligrosa que el robo de datos.[3]

En este momento, esta desconfianza no es demasiado grande. Aún podemos ignorar los riesgos y confiar en esos Gobiernos y empresas, o al menos actuar como lo hacemos, porque no tenemos muchas opciones. Pretendemos que nuestra página de Facebook esté llena de publicaciones de amigos, y no de anuncios de pago introducidos en nuestras comunicaciones personales. Fingimos que nuestros motores de búsqueda no están siendo manipulados por algoritmos que promocionan subrepticiamente productos comerciales. Esperamos que las empresas a las que se confían nuestros datos no los utilicen en contra de nuestros intereses. Aceptamos todo esto porque en realidad no tenemos otra opción. Ignoramos todo el secreto porque el secreto genera sospechas.

Hasta ahora ha funcionado. Usamos nuestros ordenadores y teléfonos, almacenamos nuestros datos en la nube, tenemos conversaciones privadas en

Facebook y mediante nuestro correo electrónico, compramos cosas por Internet, compramos y usamos cosas conectadas a Internet, y no lo pensamos demasiado.

Esto podría cambiar en cualquier momento. Y, si lo hace, va a ser malo. Los efectos negativos de vivir en una sociedad de baja confianza son considerables. Las economías sufren. La gente sufre. Todo sufre.

En 2011 publiqué *Liars and Outliers: Enabling the Trust That Society Needs to Thrive* (*Mentirosos y valores atípicos*), que analizaba la seguridad desde la perspectiva de la confianza.[4] Los sistemas de seguridad son mecanismos para reforzar la confianza: garantizan que las personas cooperen entre sí y hagan lo que se espera de ellas. De manera informal, hacemos que se cumpla internamente mediante nuestros propios códigos morales, y externamente al aprender y recordar la reputación de los demás. De manera más formal, logramos que se cumpla mediante leyes, normas y sanciones. Y lo aplicamos con tecnologías de seguridad como vallas, cerraduras, cámaras de seguridad, auditorías e investigaciones.

En el capítulo 4 decía que cualquier entidad desea tu seguridad por encima de todo excepto respecto a ella misma. Esto no es sostenible. A largo plazo, la vigilancia masiva del Gobierno no es sostenible; tenemos que limitarla si queremos un Internet fiable y, por extensión, una sociedad fiable.

El capitalismo de vigilancia no es sostenible.[5] También tenemos que limitarlo si queremos un Internet fiable. Mientras la vigilancia sea el modelo de negocios de Internet, las compañías a las que les confíes tus datos y capacidades nunca apoyarán del todo que estés seguro. Tomarán decisiones de diseño que debiliten tu seguridad tanto contra delincuentes como contra Gobiernos. Necesitamos cambiar la estructura de Internet para que este no les proporcione a los Gobiernos las herramientas para construir un estado totalitario. Esto no va a ser fácil, y no va a suceder dentro de la década, ni siquiera está claro cómo podría ocurrir en Estados Unidos: los problemas de libertad de expresión dificultarán cualquier esfuerzo legislativo por limitar la vigilancia comercial. Aun así, creo que al final llegará. Quizá el cambio sea impulsado por normas cambiantes. Estamos empezando a irritarnos por la incesante obtención de datos tanto de nuestra vida pública como privada; datos disponibles tanto para gobiernos como para corporaciones, pero no para nosotros. El capitalismo de vigilancia es un daño generalizado a la sociedad que, tarde o temprano, exigirá una reforma.

Para que las empresas y los Gobiernos tengan tu confianza, ellos deben ser fiables. Esto respalda gran parte de lo que decía en el capítulo 9. No es

suficiente con que los Gobiernos antepongan la defensa a la ofensa, sino que sus prioridades deben ser evidentes; el secreto gubernamental y las dobleces dañan la confianza.

No es suficiente con que las empresas protejan sus sistemas; deben hacerlo de manera transparente para que se vea que trabajan por el beneficio de la gente, y no que están abusando de sus posiciones de poder. Cada sugerencia en este libro debe implementarse y aplicarse de manera pública: las normas deben estar disponibles, los detalles de las infracciones deben divulgarse, el cumplimiento y las multas deben ser públicas. No se puede confiar en un Internet+ inseguro, pero un Internet+ seguro debe ser público para que se pueda confiar en él.

Todas las sugerencias que aparecen en este libro pretenden llevarnos hacia un Internet que sea fundamentalmente fiable, en el que se impida a los actores más poderosos atacar a los confiados usuarios comunes. Tenemos mucho trabajo por hacer para llegar hasta allí, y el objetivo en sí puede parecer un poco utópico; pero, mientras estamos en ello, debemos hablar de otros dos atributos clave del Internet ideal en el que estamos trabajando: la resistencia y, por último, la paz.

UN INTERNET RESILIENTE

De acuerdo con la teoría de la complejidad del sociólogo Charles Perrow, los sistemas complejos son menos seguros que los más simples y, como resultado, los ataques y accidentes que involucran sistemas complejos son más frecuentes y más dañinos. Pero Perrow demuestra que no toda la complejidad es igual. En particular, los sistemas complejos que son no lineales y estrechamente acoplados son más frágiles.[6]

Por ejemplo, el sistema de control de tráfico aéreo es un sistema acoplado de forma débil. Tanto las torres de control de tráfico aéreo individuales como los aviones tienen fallos todo el tiempo, pero, debido a que las diferentes partes del sistema solo afectan a las otras ligeramente, los resultados rara vez son catastróficos. Sí, puedes leer los titulares sobre el caos generado en este o aquel aeropuerto como resultado de problemas con los ordenadores, pero rara vez lees sobre aviones que se estrellan contra edificios, montañas o entre ellos.

Una fila de fichas de dominó de pie es un sistema lineal. Cuando una se cae, golpea la siguiente y hace que se caiga. Aunque estas cadenas son largas, se caen de una manera ordenada.

Internet es lo contrario: es no lineal, en el sentido de que las piezas pueden tener efectos desproporcionadamente raros entre sí, y a la vez estrechamente acoplado, en la medida en que estos efectos se acumulan de inmediato, características que hacen que las catástrofes sean mucho más probables. Es tan complejo que nadie entiende todo acerca de cómo funciona. Es tan complejo que apenas funciona. Es tan complejo que en muchos casos no podemos predecir cómo funcionará.

Necesitamos mayor seguridad en nuestros sistemas sociotécnicos a gran escala, pero sobre todo que sea más resistente.

Durante mucho tiempo me ha gustado el término *resiliencia*. Si miras a tu alrededor, verás que se emplea en psicología humana, en la teoría organizacional, en la recuperación de desastres, en los sistemas ecológicos, en las ciencia de materiales y en la ingeniería de sistemas. En un libro de 1991 de Aaron Wildavsky llamado *Searching for Safety* (*En busca de la seguridad*), encontramos la siguiente definición: «La resiliencia es la capacidad de hacer frente a peligros no anticipados y, una vez que se han manifestado, aprender a recuperarse».[7]

He estado hablando sobre la resiliencia en la seguridad de TI durante más de quince años.[8] En mi libro de 2003, *Beyond Fear* (*Más allá del miedo*), le dediqué varias páginas a la resiliencia. Decía lo siguiente:

> Los buenos sistemas de seguridad son resilientes. Pueden soportar fallos. Un solo fallo no causa una cascada de más fallos. Pueden soportar ataques, incluyendo atacantes que hacen trampa. Pueden soportar nuevos avances en tecnología. Pueden fallar y recuperarse del fracaso.[9]

En 2012, el Foro Económico Mundial describió la resiliencia cibernética como una capacidad habilitadora que proporciona seguridad física, seguridad económica y una ventaja comercial competitiva.[10]

En 2017, el Consejo Nacional de Inteligencia de Estados Unidos, que forma parte de la Oficina del Director de Inteligencia Nacional, publicó un documento completo que analiza las tendencias de seguridad a largo plazo en el que se hablaba de resiliencia:

> Las sociedades más resilientes serán aquellas que desencadenarán y abarcarán todo el potencial de todos los individuos (ya sean mujeres y minorías o aquellos golpeados por las recientes tendencias económicas y tecnológicas). Se moverán con las corrientes históricas, en vez de en

> contra, haciendo uso del alcance cada vez mayor de la habilidad humana para dar forma al futuro. En todas las sociedades, incluso en las circunstancias más sombrías, habrá quienes elijan mejorar el bienestar, la felicidad y la seguridad de los demás empleando tecnologías transformadoras para hacerlo a gran escala. Si bien también ocurrirá lo contrario (las fuerzas destructivas se potenciarán como nunca), el enigma central para los Gobiernos y las sociedades es cómo combinar las dotaciones individuales, colectivas y nacionales de una manera que proporcione seguridad sostenible, prosperidad y esperanza.[11]

Táctica y tecnológicamente, la resiliencia significa muchas cosas diferentes: múltiples capas de defensa, aislamiento, redundancia, etc. Necesitamos ser resilientes también como sociedad. Gran parte del daño causado por los ataques cibernéticos es psicológico. Rusia interrumpió el suministro de energía eléctrica en Ucrania dos veces, y ahora los ciudadanos ucranianos deben vivir con el conocimiento de que su acceso a la electricidad es frágil. Una red eléctrica más resistente significaría una sociedad más resiliente.

Podemos prevenir algunos ataques, pero tenemos que detectar y responder al resto de ellos después de que ocurran. Así es como logramos la resiliencia. Era así hace quince años y, en cualquier caso, todavía lo es hoy.

UN INTERNET DESMILITARIZADO

En el capítulo 4 decía que estamos en una batalla en medio de una guerra cibernética. Las batallas son siempre caras y están alimentadas por la ignorancia y el miedo: ignorancia de las capacidades de nuestros enemigos y temor de que las suyas sean mayores que las nuestras. Todo esto se magnifica en el ciberespacio. ¿Recuerdas lo difícil que fue para Estados Unidos discernir cuáles eran las capacidades de las armas nucleares y químicas en Irak? Las capacidades cibernéticas son incluso más fáciles de ocultar.

Esta batalla perjudica nuestra seguridad de dos maneras. Primero, reduce de inmediato la seguridad al dejar que Internet+ permanezca desprotegido. Mientras haya países que necesiten vulnerabilidades para sus armas cibernéticas y estén dispuestos a descubrirlas o comprarlas a otros, habrá vulnerabilidades que no se repararán.

En segundo lugar, aumenta las posibilidades de una guerra cibernética. Las armas piden ser usadas, y cuantas más armas haya en el mundo, mayor será el riesgo de que se usen. El carácter perecedero inherente a las armas

cibernéticas que mencionaba en el capítulo 4 hace que resulten atractivas de usar. La naturaleza ofensiva de los preparativos en el campo de batalla aumenta la posibilidad de represalias, incluso aunque se basen en un malentendido. Y el vacío de atribuciones aumenta la posibilidad de malentendidos y de engaños deliberados, en especial para los países que no tienen conocimiento de las capacidades de inteligencia de Estados Unidos.

Necesitamos trabajar para desmilitarizar Internet. Puede parecer imposible, y en el clima geopolítico actual podría serlo, pero sin duda es algo alcanzable a largo plazo.

Un comienzo sería ir más allá de las metáforas militares para la seguridad de Internet. Por ejemplo, conceptualizarla como un problema de higiene o contaminación pública nos llevará a diferentes tipos de soluciones. Un informe de 2017 realizado por el Grupo de Trabajo Cibernético de Nueva York sugirió que los Gobiernos podrían gravar las *emisiones* dañinas de los ISP (malware, tráfico DDoS, etc.) e incluso implementar algún tipo de régimen de limitaciones y de comercio.[12] Las leyes internacionales relacionadas con la contaminación también podrían servirnos como comparación útil para los problemas de seguridad internacional en Internet+.[13]

Incluso más que cualquiera de estas dos cosas necesitamos crear un Internet+ pacífico. El término *paz cibernética* se ha mostrado como una alternativa a la retórica cada vez más militar sobre el ciberespacio. El profesor de Derecho en Ciberseguridad Scott Shackelford, de la Universidad de Indiana, ha tratado de definir este nebuloso término:

> La paz cibernética no es la ausencia de ataques o abusos, una idea que podría llamarse paz cibernética negativa. Más bien, es una red de regímenes multinivel que trabajan juntos para promover la ciberseguridad global, justa y sostenible, que ayuda a aclarar las normas para que las empresas y los países ayuden a reducir el riesgo de conflictos, delincuencia y espionaje en el ciberespacio a niveles comparables con los de otros negocios y empresas nacionales. Trabajando juntos a través de asociaciones policéntricas, y con el liderazgo de individuos e instituciones comprometidos, podremos detener la guerra cibernética antes de que comience, sentando las bases para una paz cibernética positiva que respete los derechos humanos, difunda el acceso a Internet y fortalezca los mecanismos de gobierno mediante el fomento de la colaboración entre los interesados.[14]

La politóloga Heather Roff está de acuerdo y sostiene que «la paz cibernética debe basarse en una concepción de paz positiva que elimine las formas estructurales de violencia» y que esté basada en cuatro factores necesarios, como «una sociedad, confianza, gobernabilidad y el libre flujo de información».[15]

En cierto modo, esto es como un Consejo de Seguridad de la ONU para Internet, y podemos aprender de los éxitos y fracasos de esa organización. Es un objetivo digno por el que deberíamos esforzarnos.

En una escala más pequeña e inmediata, hay formas en las que podemos trabajar para promover un Internet más justo y equitativo en este momento. Por todos los problemas con el Gobierno y la vigilancia corporativa que tenemos en Estados Unidos y en otras democracias occidentales, y por todos los peligros que se avecinan para nuestras vidas y libertades y sobre los que he estado hablando, es importante recordar que miles de millones de personas disfrutan de una libertad digital considerablemente menor que nosotros y se enfrentan a riesgos mucho más graves como resultado del uso de Internet en países como Egipto, Etiopía, Myanmar y Turquía.

Estoy en el consejo de una organización llamada Access Now. Nuestra misión es defender y ampliar los derechos digitales de los usuarios en riesgo de todo el mundo. Uno de los servicios que ofrecemos es una línea de ayuda de seguridad digital que ofrece asistencia técnica a las personas que creen que son víctimas de la vigilancia gubernamental. También proporcionamos análisis políticos y promovemos propuestas gubernamentales por todo el mundo, abogamos por cambiar las políticas actuales en diferentes países y convocamos una conferencia anual sobre derechos humanos en la era digital.

He tenido en mente esta organización y su trabajo mientras escribía este libro. Tanto los problemas como las soluciones de las que he estado hablando se centran en las democracias liberales del mundo. No se aplican a los países que utilizan Internet para encontrar y detener a disidentes o para arrestar a personas que imparten formación en seguridad a disidentes. Aun así, las recomendaciones que he formulado también tendrían un efecto positivo en ellas, incluso aunque solo las democracias las sigan. Mientras tanto, existen personas y grupos, como Access Now, que escriben y trabajan para defender los derechos digitales de estos usuarios de alto riesgo.

A menudo se habla de Internet como un ecualizador social, y esa es una caracterización justa. Circula y amplifica ideas importantes e ideales humanos, conecta a las personas por encima de las fronteras y ha provocado y permitido una docena de revoluciones al nivel de la gente de la calle lideradas

por personas que buscan mayores libertades y un futuro mejor. ¿Quién sabe cuál puede ser el potencial positivo de Internet+? Por supuesto que Internet también tiene un punto débil, y he hablado largo y tendido en este libro sobre los problemas que nos acechan en esos frentes. Pero, igual que con la mayoría de los esfuerzos humanos, debemos continuar trabajando para que el emergente Internet+ se convierta en un medio que incorpore y permita que los ideales humanos de confianza, seguridad, resiliencia, paz y justicia puedan existir.

CONCLUSIÓN
Unamos la tecnología con las políticas

VUELVO REPETIDAMENTE A TRES ESCENARIOS en este libro. El primero es un ciberataque contra una red eléctrica. El segundo es el asesinato al piratear por control remoto un automóvil conectado a Internet. El tercero es el escenario de «haz clic aquí para matarlos a todos», que involucra la replicación de un virus letal por una bioimpresora hackeada. El primer ejemplo ya tuvo lugar. El segundo, como se ha demostrado, es posible. El tercero está por llegar.

Dan Geer, un experto en seguridad, advirtió una vez lo siguiente: «Una tecnología que puede darte todo lo que deseas es una tecnología que puede quitarte todo lo que tienes».[1] Los beneficios de Internet para la sociedad han sido, y seguirán siendo, enormes. Ya ha transformado nuestras vidas para mejor en una multitud de formas, y tras unas pocas décadas es difícil imaginar volver al lugar en el que estuvimos alguna vez. Los futuros avances de Internet+ serán aún más transformadores: en los sensores y en los controladores, en los algoritmos y los datos, en la autonomía y en los sistemas ciberfísicos, en la inteligencia artificial y en la robótica. Esto hará que nuestra sociedad sea tan irreconocible para nosotros hoy como lo sería la sociedad moderna para alguien de la Europa anterior a la Ilustración. Estamos viviendo un momento increíble, y envidio a las generaciones más jóvenes que tienen todavía más futuro por delante.

Pero los riesgos y los peligros son igualmente transformadores. Internet+ afecta al mundo de una manera física directa, y esto tiene implicaciones grandes y pequeñas. Al unir todo en un solo sistema complejo e hiperconectado, los riesgos se vuelven rápidamente catastróficos.

Mientras tanto, todas nuestras leyes, reglas y normas se basan en un Internet nocivo. Eso es lo que ha cambiado, y esa es la realidad a la que debemos responder presionando a los Gobiernos para que actúen.

Parte de mi pesimismo surge de la extrapolación de las tecnologías. Tendemos a extrapolar el mundo de hoy con solo algunos cambios importantes. Mi ejemplo favorito proviene de la película de 1982 *Blade*

Runner, que presenta androides tan avanzados que son imposibles de identificar sin un equipo especializado. Sin embargo, cuando Deckard (el personaje de Harrison Ford) quiere conocer a uno de ellos, utiliza un teléfono público que funciona con monedas porque en ese momento todavía no se podían imaginar los teléfonos móviles.[2]

También tendemos a sobrevalorar los efectos a corto plazo del cambio tecnológico y a subestimarlos a largo plazo.[3] Piensa en los primeros años de Internet. Mucha gente se dio cuenta de que se usaría para comprar y vender cosas, pero nadie previó eBay. Mucha gente entendió que los amigos lo usarían para mantenerse en contacto, pero nadie pronosticó Facebook. Una y otra vez, anticipamos los usos inmediatos de una nueva tecnología, pero no comprendemos cómo se manifestará en la sociedad. Veo que sucede lo mismo con los asistentes digitales personales, con los robots, con las tecnologías de criptomonedas, como bitcóin, con la inteligencia artificial y con los coches sin conductor.

Esto significa que es fácil caer en la trampa del determinismo técnico. Puedo trazar con facilidad las trayectorias actuales de seguridad. Sin embargo, no tengo ni idea de qué nuevos e innovadores descubrimientos e invenciones aparecerán dentro de tres, cinco o diez años, no puedo predecir qué avances fundamentales en las ciencias de la computación modificarán de manera irrevocable el equilibrio entre ataque y defensa, no puedo prever qué otras tecnologías podrían inventarse que alteren profundamente la seguridad de Internet+, ni puedo saber qué tipo de cambios sociales y políticos podrían ocurrir que hagan que los riesgos de los que hemos hablado en este libro sean menos importantes, más manejables o del todo irrelevantes. Nuestra imaginación colectiva falla porque el futuro es, en el fondo, inimaginable.

Aun así, creo que nuestras soluciones de seguridad de Internet+ están delante de nosotros, y no detrás. Es mucho más probable que diseñemos una manera de solucionar los problemas a los que nos enfrentamos que el hecho de que no haya escapatoria. A pesar de mis recomendaciones del capítulo 6, es poco probable que tengan éxito las soluciones que nos obligan a restringir significativamente la omnipresencia de los ordenadores, de Internet o de cualquier otra de las tecnologías analizadas en este libro. Los beneficios de estas tecnologías son demasiado grandes, y en la actualidad tenemos una pobre visión de futuro para permitir que algo se interponga en el camino.

Tenemos que apostar más por la investigación, las ideas, la creatividad y la tecnología. No hay escasez de ideas: ya sean significativas, progresivas,

profundas o revolucionarias. Y aunque desconozca cómo serán las soluciones, confío plenamente en que existen.

Por ejemplo, veo una gran promesa en las tecnologías de inteligencia artificial y aprendizaje automático. En resumen, parte de la razón por la que el ataque es más fácil que la defensa es que los atacantes deciden la naturaleza de sus ataques, pueden usar las fortalezas relativas de las personas y los ordenadores, y apuntar a sus debilidades relativas. Las tecnologías de inteligencia artificial prometen alterar este equilibrio entre los ordenadores y las personas, tanto en la ofensiva como en la defensa. Esto disminuirá las ventajas relativas para el atacante que le proporcionan la velocidad, la sorpresa y la complejidad.[4]

Mi pesimismo se debe más a la incapacidad colectiva de Estados Unidos para imaginar al Gobierno como una fuerza por el bien del mundo. Cuando reviso el panorama de seguridad de Internet actual, veo un entorno moldeado por decisiones corporativas que quieren maximizar las ganancias y la renuncia por parte del Gobierno a ejercer su función reguladora para proteger a todos los ciudadanos. Veo a una población hipnotizada por las capacidades francamente asombrosas de estas nuevas tecnologías en red y negligente al considerar las repercusiones sociales tan profundas de todo esto. Nuestro nivel actual de seguridad está determinado por el mercado, y sé (y espero haberlo demostrado) que será inadecuado para Internet+.

Por eso paso tanto tiempo pensando en las políticas del Gobierno. Quiero estar listo con propuestas antes de que estalle una crisis. En una crisis, el Congreso deberá emprender acciones y, sin duda, empleará ese falso silogismo que dice lo siguiente: «Se debe hacer algo. Esto es algo. Por lo tanto, debemos hacerlo». Es importante hablar ahora sobre cómo serán las buenas políticas de seguridad de Internet+, cuando tenemos tiempo para hacerlo lenta y cuidadosamente, y antes de que ocurra una catástrofe.

En este libro defiendo el buen Gobierno que hace el bien. Puede ser una postura difícil de defender, pues existe un gran potencial para que el Gobierno sea ineficaz o incluso perjudicial, pero no veo ninguna otra opción. Si el Gobierno renuncia a sus responsabilidades, como se ha hecho en gran parte de Estados Unidos hasta la fecha, terminaremos con un Internet+ inseguro que solo sirva a los intereses comerciales y militares a corto plazo.

A pesar del pesimismo que destila una gran parte de este libro, soy optimista sobre la ciberseguridad a largo plazo. Al final, daremos con la solución.

Otto von Bismarck observó lo siguiente: «La política es el arte de lo posible».[5] A eso le respondo: La tecnología es la ciencia de lo posible. Pero la política y la tecnología ofrecen diferentes posibilidades, y entender esto es darse cuenta de que los políticos y los tecnólogos definen *posible* de maneras diferentes. Como tecnólogo, quiero llegar a la respuesta correcta o a la mejor solución para un problema. Un político, por otro lado, es pragmático, no busca lo que es correcto o lo mejor, sino lo que puede lograr.

Hoy en día, la tecnología y la política están íntimamente entrelazadas. Los escenarios que he descrito, las tendencias tecnológicas y económicas que los causaron y los cambios políticos necesarios para solucionarlos provienen de mis años de participación en el desarrollo de políticas y de tecnología de seguridad de Internet. Comprender ambas cosas es algo fundamental.

Durante las últimas dos décadas, hemos visto muchas recomendaciones equivocadas para las políticas de seguridad de Internet. Los ejemplos incluyen la insistencia del FBI de que los dispositivos informáticos estén diseñados para facilitar el acceso del Gobierno a fin de repeler el error de *oscurecerse*, el proceso de vulnerabilidad mediante el cual los organismos gubernamentales determinan si divulgar y corregir las vulnerabilidades o usarlas para atacar otros sistemas, el fallo de las máquinas de votación con pantalla táctil sin papel para producir elecciones fiables y la DMCA. Si seguiste alguno de estos debates sobre políticas a medida que se desarrollaban, solo escuchaste a los políticos y tecnólogos hablar entre ellos.

Hemos visto esto en los capítulos 6, 7, 8 y 9 un montón de ideas geniales que no sucederán pronto. Y vimos la contraparte de esto en el capítulo 11: lo que los legisladores que no saben de tecnología podrían hacer para empeorar las cosas.

Internet+ agravará estos problemas. La creciente división entre Washington y Silicon Valley es peligrosa (la desconfianza mutua entre Gobiernos y empresas tecnológicas). A medida que los problemas de seguridad informática se extienden a otras industrias, veremos desconexiones similares entre tecnología y política, y entre tecnólogos y legisladores. El abogado británico Nick Bohm lo expresó con elocuencia cuando hablaba de «los abogados e ingenieros cuyos argumentos pasan a través de ellos como fantasmas enfadados».[6]

Esta división no es nueva. Al tomar la palabra en la Conferencia de Seguridad de Múnich en 2014, el presidente de Estonia Toomas Hendrik Ilves observó:

> Creo que gran parte del problema al que nos enfrentamos hoy

> representa la culminación de un problema diagnosticado hace cincuenta y cinco años por C. P. Snow en su ensayo *Las dos culturas*: la ausencia de diálogo entre las tradiciones científico-tecnológicas y las humanistas. Cuando Snow escribió su ensayo clásico se lamentó de que ninguna cultura entendiera o incidiera en la otra. Hoy, desprovistos de la comprensión de los temas y de los escritos fundamentales en el desarrollo de la democracia liberal, los expertos en computación idean formas cada vez mejores de controlar a las personas… simplemente porque pueden y es genial. Los humanistas, por otro lado, no entienden la tecnología subyacente y están convencidos, por ejemplo, de que el seguimiento de los metadatos significa que el Gobierno lee los suyos. Las dos culturas de C. P. Snow no solo no se hablan entre sí, sino que actúan como si la otra no existiera.[7]

Esto podría aceptarse en 1959, porque la tecnología y la política no interactuaban entre sí tanto como lo hacen ahora. Hoy en día sí que lo hacen. Los contratiempos tecnológicos pueden tener consecuencias catastróficas. Es hora de arriesgarse. Los legisladores y los tecnólogos necesitan trabajar juntos; necesitan aprender los idiomas de cada uno y educarse mutuamente.

La solución a esto tiene dos partes. La primera: los responsables políticos deben entender de tecnología. En mi mundo de fantasía, las decisiones políticas se parecen a las de *Star Trek: La siguiente generación*. Allí, todos se sientan alrededor de una mesa de conferencias y los tecnólogos explican el significado de los datos y las realidades científicas al capitán Picard, quien escucha, considera los hechos y sus opciones, y luego toma una decisión basada en la ciencia y en la tecnología.

Pero no funciona así en el mundo real. Con demasiada frecuencia los políticos no entienden ni de ciencia ni de tecnología. Muy a menudo tienen sus planes e ideas preconcebidas y tratan de obligar a la ciencia a encajar; a veces incluso se jactan de no entender de tecnología. Los grupos de presión se complacen al proporcionar pseudociencias que coincidan con cualquier política, y tienen tantas obligaciones que no tienen tiempo para comprender por completo la información que se les presenta.

En el capítulo 11 mencionaba los intentos de Australia de legislar sobre las puertas traseras en los sistemas de seguridad. Respondiendo a una pregunta de la prensa en 2017, el primer ministro Malcolm Turnbull dijo: «Bueno, las leyes de Australia prevalecen en Australia, les puedo asegurar eso. Las leyes de las matemáticas son muy encomiables, pero la única ley que se aplica en Australia es la ley de Australia».[8] Esta afirmación, por supuesto,

es ridículamente errónea y fue objeto de burlas generalizadas y justificadas. Cuando las leyes de Australia y de las matemáticas se contradigan, las leyes de las matemáticas prevalecerán siempre.

Del mismo modo, no creo que la mayoría de los responsables de la formulación de políticas comprendan del todo los riesgos que plantean las grandes bases de datos corporativas que contienen nuestra información personal o las amenazas a la infraestructura crítica de nuestro país, tanto de piratas informáticos como de Estados nación. Tampoco creo que entiendan los conceptos fundamentales de seguridad informática que enumeraba en el capítulo 1 o los fallos analizados en los capítulos 2 y 3.

Las políticas deben tener en cuenta las matemáticas, la ciencia y la ingeniería; no deben pretender que las cosas verdaderas no lo sean ni que sea cierto lo que no lo es. Considero que la política es el mecanismo principal para abordar nuestros problemas de seguridad informática. Todos nuestros problemas en las políticas de seguridad tendrán componentes tecnológicos sólidos, pero nunca conseguiremos las políticas adecuadas si los responsables de su formulación se equivocan con la tecnología. No se trata de convertir a los responsables políticos en tecnólogos, sino de garantizar que tengan una intuición tecnológica que los ayude a comprender a los tecnólogos y a tomar decisiones sobre tecnología. La ignorancia ya no es una opción.

Dicho esto, por más importante que sea que los responsables de las políticas entiendan de tecnología, eso no será suficiente. La segunda parte para resolver la brecha entre tecnología y política es que los tecnólogos se involucren en la política. No todos, por supuesto, pero necesitamos más tecnólogos con intereses públicos como estas personas:

Latanya Sweeney dirige el Laboratorio de Privacidad de Datos en Harvard, donde es profesora de Gobierno y Tecnología. Probablemente sea la mejor analista de identificación del anonimato que con frecuencia demuestra cómo las diferentes técnicas de anonimato no funcionan.[9] También expuso sesgos en los algoritmos de Internet[10] y ha hecho contribuciones significativas a las tecnologías de privacidad.[11] En 2014, pasó un año como tecnóloga principal en la Comisión Federal de Comercio.

Susan Landau es en la actualidad profesora de Ciberseguridad en la Universidad de Tufts. Es criptógrafa y tecnóloga de seguridad informática, y ha trabajado en Sun Microsystems y en Google. Quizá sea hoy en día la mejor pensadora y comunicadora que tenemos sobre el valor del cifrado ubicuo frente a los temores de *oscurecimiento* del FBI; ha escrito libros y artículos, [12] y ha testificado ante el Congreso sobre estos temas.[13]

Ed Felten es un profesor de Ciencias Informáticas de Princeton que ha realizado considerables investigaciones de seguridad en una variedad de áreas. Tal vez sea más conocido por su análisis de la seguridad en las máquinas de votación electrónica.[14] En 2010, lo nombraron tecnólogo jefe de la Comisión Federal de Comercio y fue director adjunto de tecnología de Estados Unidos de 2015 a 2017.

Podría llenar este capítulo con nombres e historias (Ashkan Soltani, Raquel Romano, Chris Soghoian y otros), pero nuestras necesidades son mucho mayores que las de los prominentes pioneros que dieron el salto desde los roles técnicos al desarrollo de las políticas de seguridad. Los tecnólogos deben impregnar la política en todos los niveles, no solo en los roles más visibles. Deben formar parte del personal legislativo, de las agencias reguladoras y de las organizaciones de control no gubernamentales, figurar entre los miembros de la prensa y entre los grupos de expertos en políticas. Necesitamos mucho más de lo que tenemos en la actualidad.

Hay programas que quieren situar a los tecnólogos en posiciones políticas. El Congreso de Tecnología es un programa de becas de Nueva América y ubica a los tecnólogos dentro del personal del Congreso. El programa Open Web Fellowship coloca a los tecnólogos dentro de organizaciones sin ánimo de lucro. Hoy en día, se centra en organizaciones que trabajan para proteger el Internet abierto y más ampliamente para servir al interés público en temas de políticas de Internet.

Otros programas intentan aprovechar la tecnología para crear políticas. Código para América (*Code for America*) se focaliza en conectar personas con habilidades de ingeniería y otras habilidades tecnológicas con los Gobiernos locales para influir en la forma en la que se diseñan e implementan los sistemas.

Electronic Frontier Foundation, de cuya junta formo parte, ha combinado durante mucho tiempo la experiencia tecnológica y la de creación de políticas, y lo mismo ocurre con el Centro de Información de Privacidad Electrónica, en cuya junta también he participado. La Unión Estadounidense por las Libertades Civiles (ACLU, por sus siglas en inglés), mediante su proyecto Discurso, Privacidad y Tecnología, se enfoca en el impacto de las libertades civiles en las nuevas tecnologías.[15] Otras organizaciones, como Human Rights Watch y Amnistía Internacional, están empezando a introducirse en esta área, aunque con más lentitud de lo que me gustaría.

Muchas universidades ahora cuentan con programas de estudios interdisciplinarios que combinan tecnología y política.[16] El MIT alberga una

iniciativa de investigación de políticas de Internet, y los cursos que imparte ofrecen a los estudiantes una comprensión integrada de la tecnología y de las políticas públicas,[17] y la Universidad de Georgetown cuenta con el Centro de Privacidad y Tecnología.[18] Muchas escuelas ofrecen grados conjuntos en Derecho y Tecnología; por ejemplo, yo enseño en la Escuela de Gobierno de Harvard Kennedy, que forma parte de su programa Digital HKS.[19]

Todos estos cursos son geniales, pero todavía son excepcionales. Necesitamos crear una trayectoria profesional viable para los tecnólogos con interés público,[20] cursos y programas de grado que combinen tecnología y política, así como prácticas, becas y trabajos a tiempo completo en organizaciones que requieran estas habilidades. Necesitamos que las compañías de tecnología ofrezcan años sabáticos al personal que quiera explorar este camino y que valoren su experiencia en políticas cuando regresen al mundo de los negocios. Necesitamos que se garantice que, aunque los recién llegados a este campo no ganen tanto como lo harían en una empresa de alta tecnología, tendrán futuros profesionales prometedores. La seguridad de nuestra sociedad informatizada y en red —es decir, la seguridad de nosotros mismos, de nuestras familias, hogares, empresas y comunidades — depende de ello.

Un buen modelo se puede encontrar en la ley de interés público.[21] A principios de la década de los setenta, realmente no existía tal cosa, pero después de que la Fundación Ford y otras organizaciones filantrópicas decidieran apoyar a los bufetes de abogados de interés público en ciernes, el número de abogados en este campo explotó. A finales de 1960, había 92 centros de derecho de interés público en Estados Unidos[22] y en el año 2000 había más de mil.[23] Hoy en día, el 20 % de los graduados de la Escuela de Derecho de Harvard accede directamente a la ley de interés público, en lugar de comenzar en un bufete de abogados o en una empresa.[24] Es una experiencia valiosa que les sirve a estos abogados en sus carreras, con independencia de sus futuros trabajos.

La informática no es así. Prácticamente ninguno de los graduados de Harvard, ni de ninguna otra universidad, se dedica a la tecnología de interés público; por lo general, no es una trayectoria profesional en la que los programadores e ingenieros piensen. No quiero culpar a los estudiantes; no hay trabajos de interés público esperándolos, ni tener experiencia en ello se convierte en un punto importante de su currículum.

Esta necesidad de combinar tecnología y política trasciende la seguridad. Casi todos los grandes debates políticos del siglo XXI involucrarán la

tecnología. Ya se trate de armas de destrucción masiva, robots, cambio climático, seguridad alimentaria o drones, comprender la política exige comprender la ciencia y la tecnología relevantes. Si no conseguimos que más tecnólogos trabajen en política, terminaremos con unas malas políticas.

De manera más general, debemos comenzar a tomar decisiones morales, éticas y políticas sobre cómo debería funcionar Internet+. Hemos construido un mundo en el que los programadores tenían el derecho inherente a codificar el mundo como querían verlo, algo que aceptamos porque lo que decidían no importaba demasiado. Ahora sí importa, y creo que este privilegio debe terminar.

Tú, lector, puedes ayudar a lograrlo. Hemos estado embelesados por la increíble promesa de estas tecnologías, y no hemos podido ver los problemas en ellas. Espero que las noticias de los últimos dos años, y el presente libro, cambien este hecho. Ahora tienes que presionar contra el *statu quo*. Anima a los cargos electos a que se tomen en serio las amenazas haciendo de la seguridad y de la privacidad de Internet+ un asunto de campaña. No les va a importar a nuestros líderes si a nosotros no nos importa.

Internet+ está llegando. Con poca previsión, arquitectura o planificación, pero está llegando. Va a cambiar todo de maneras que solo podemos imaginar y de maneras que aún no somos capaces de imaginar. También cambiará la seguridad: más autonomía, más consecuencias en el mundo real, menos interruptores y más riesgos catastróficos.

Viene más rápido de lo que la mayoría de nosotros pensamos, y sin duda demasiado rápido como para estar preparados con las herramientas que tenemos ahora. Necesitamos hacerlo mejor: adelantarnos y empezar a tomar decisiones. Necesitamos comenzar a construir sistemas de seguridad tan robustos como las amenazas. Necesitamos leyes y políticas que aborden las amenazas, la economía y la psicología de manera adecuada, y que no se vuelvan obsoletas con las tecnologías cambiantes.

Nuestra única esperanza de llegar ahí es reunir a tecnólogos y políticos en la mítica sala de reuniones de *Star Trek* para resolver esto. Ahora.

AGRADECIMIENTOS

Después de una docena de libros, tal vez pienses que ya tengo bastante interiorizado este proceso; aun así, cada uno es diferente. Empecé este libro demasiado pronto después de *Data y Goliat* y, como resultado, tuve algunos falsos inicios. Comencé a escribir el libro que acabas de leer en el verano de 2017 y lo envié para su publicación a finales de marzo de 2018.

Cuento con un excelente equipo de personas que han trabajado conmigo en mis últimas obras, y todos volvieron a reunirse también para este libro. Kathleen Seidel es una investigadora extraordinaria con buen ojo para la prosa, tanto en lo macro como en lo micro. Beth Friedman ha corregido todo lo que he escrito durante veinte años, me conoce a mí y mi estilo de escritura, y no sé cómo me las arreglaría sin ella. No solo editó el libro antes de enviárselo a la editorial, sino que también trabajó con su editor interno para que yo no tuviera que hacerlo. Por último, Rebecca Kessler proporcionó una revisión de contenido muy necesaria al final del proceso de escritura; su ayuda también es inestimable. A ellas tres se suma Katherine Mansted, quien intervino en las últimas etapas para proporcionar investigación adicional y aplicó su gran capacidad de síntesis.

Muchas personas leyeron y comentaron todo o parte del borrador del manuscrito. Cada error que encontraron y cualquier pensamiento difuso que marcaron mejoró el libro. Estas personas fueron Michael Adame, Ross Anderson, Steve Bass, Michael Brennan, John Bruce, Cody Charette, John Davis, Judith Donath, Nora Ellingsen, Mieke Eoyang, Greg Falco, Hubert Feyrer, John Fousek, Brett Frischmann, Blair Ganson, Jason Giffey, Jack Goldsmith, Chloe Goodwin, Sarah Grant, Eldar Haber, Bill Herdle, Trey Herr, Christopher Izant, Andrei Jaffe, Danielle Kehl, Eliot Kim, Xia King, Jonathan Korn, Nadiya Kostyuk, Alexander Krey, Lydia Lichlyter, Aleecia McDonald, Daniel Miessler, Adam Montville, David O’Brien, Christen Paine, David Perry, Stuart Russell, Martin Schneier, Nick Sinai, Nathaniel Sobel, Hannah Solomon-Strauss, Lance Spitzner, Stephen Taylor, Marc van Zadelhoff, Arun Vishwanath, Sara M. Watson, Jarad Webber, Tom Wheeler y

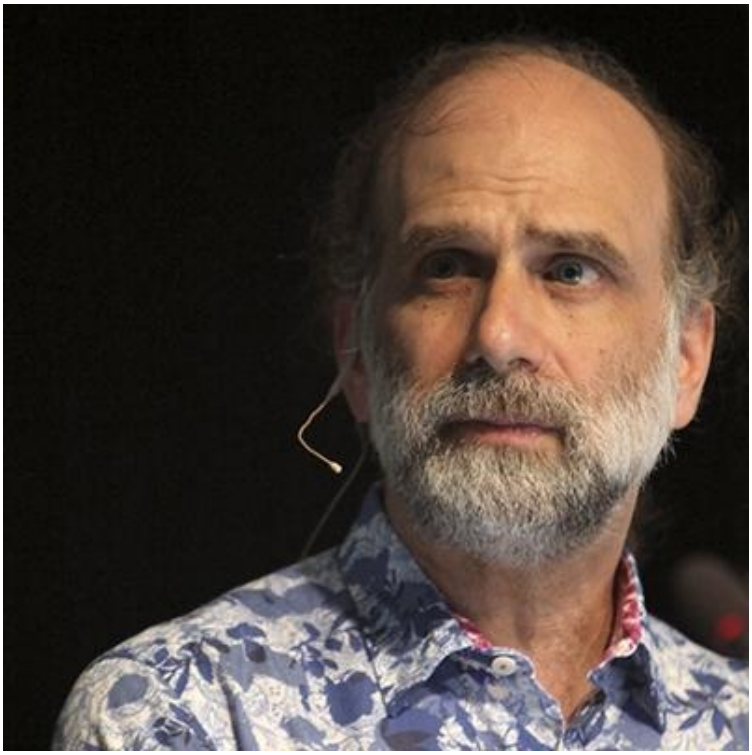
Ben Wizner. No es exagerado decir que este sería un libro mucho peor sin ellos.

W. W. Norton sigue siendo una editorial excelente y me gustaría darle las gracias a mi editor de mesa original Jeff Shreve, así como a Brendan Curry, quien se hizo cargo de todo cuando aquel se fue. Jeff firmó el contrato demasiado pronto y fue paciente cuando no pude respetar la fecha de entrega. Sé que es un cliché decir que mi editor nunca perdió la fe en mí, y, para ser sincero, no tengo idea de lo que pasaba por su cabeza, pero *afirmó* que nunca había perdido su fe en mí, y nunca quiso que le devolviera el anticipo, ni siquiera cuando se lo ofrecí. Brendan Curry lo tuvo más fácil; cuando él apareció, en realidad yo ya estaba avanzando. Su trabajo en el proceso de publicación fue ejemplar, sobre todo mientras yo presionaba a Norton para que abreviara el plazo.

Asimismo, Susan Rabiner sigue siendo una agente excelente. Si solo se tratara de negociar un contrato, cualquiera podría hacerlo, pero me sorprende continuamente lo importante que es tener a alguien entre el editor y yo.

También me gustaría agradecer la ayuda de la Universidad de Harvard, en concreto la del Centro Berkman Klein para Internet y la Sociedad, la del Proyecto de Ciberseguridad del Centro Belfer para la Ciencia y los Asuntos Internacionales, y la de la Escuela de Gobierno de Harvard Kennedy, en general, por facilitarme un hogar para escribir, hablar y enseñar. Valoro a mis colegas y amigos en esas instituciones, y sus ideas e ideales están presentes en este libro. En Cambridge me gustaría darle las gracias a mi empleador principal, Resilient Systems, que se convirtió en IBM Resilient y que pronto formará parte de IBM Security, por darme rienda suelta para escribir y publicar este libro, y por no pedirles ni una vez a sus abogados que se lo leyeran. Me gustaría agradecerle a Norton haber publicado el libro que quería publicar, a pesar de las preocupaciones de sus abogados.

Y, por último, me gustaría agradecerles a mi esposa desde hace veintiún años, Karen Cooper, y a todos mis amigos y colegas haberme aguantado mientras escribía este libro. Tiendo a tener una relación codependiente con los manuscritos; cuando les va bien, estoy bien, pero cuando tienen problemas, estoy triste. Como con todos los libros, este tuvo sus momentos. Les agradezco a todos su paciencia y su amabilidad.



BRUCE SCHNEIER (15 de enero de 1963, Nueva York, Nueva York, Estados Unidos). Apodado «el gurú de la seguridad» digital por *The Economist*, Bruce Schneier es posiblemente el criptógrafo más reconocido de Estados Unidos. Autor de una decena de libros en materia de seguridad informática, más de doscientas cincuenta mil personas leen sus influyentes *newsletter Crypto-Gram* y blog *Schneier on Security*. Además, ha testificado ante el Congreso de Estados Unidos, ha participado en varios comités gubernamentales y aparece frecuentemente en televisión. Entre las instituciones con las que colabora destacan la Universidad de Harvard e IBM. *Haz clic aquí para matarlos a todos* es su último trabajo.

NOTAS

[1] Un vídeo muestra la expresión aterrorizada del conductor: GREENBERG, Andy. «Hackers remotely kill a Jeep on the highway with me in it». *Wired* (21 de julio de 2015). <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>, <https://www.youtube.com/watch?v=MK0SrxBC1xs> (vídeo). <<

[2] GREENBERG, Andy. «The Jeep hackers are back to prove car hacking can get much worse». *Wired* (1 de agosto de 2016). <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks> <<

[3] ROUF, Ishtiaq *et al*. «Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study». *19 th USENIX Security Symposium* (12 de agosto de 2010). <http://winlab.rutgers.edu/~gruteser/papers/ccs308-baik.pdf> <<

[4] FINKLE, Jim; WOODALL, Bernie. «Researcher says can hack GM's OnStar app, open vehicle, start engine». *Reuters* (30 de julio de 2015). <http://www.reuters.com/article/us-gm-hacking-idUSKCN0Q42FI20150730> <<

[5] ROUF, Ishtiaq *et al*. «Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study». 19th USENIX Security Symposium (12 de agosto de 2010). <http://www.winlab.rutgers.edu/~Gruteser/papers/xu_tpms10.pdf> <<

[6] ZETTER, Kim. «Feds say that banned researcher commandeered plane». *Wired* (16 de junio de 2016). <https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane> <<

[7] GROBART, Sam. «Hacking an airplane with only an Android phone». *Bloomberg* (12 de abril de 2013). <http://www.bloomberg.com> <<

[8] BIESECKER, Calvin. «Boeing 757 testing shows airplanes vulnerable to hacking, DHS says». *Aviation Today* (8 de noviembre de 2017). <http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says> <<

[9] ZETTER, Kim. «The malware used against the Ukrainian power grid is more dangerous than anyone thought». *Vice Motherboard* (12 de junio de 2017). <https://motherboard.vice.com/en_us/article/zmeyg8/ukraine-power-grid-malwarecrashoverride-industroyer>. POULSEN, Kevin. «U.S. power companies warned 'nightmare' cyber weapon already causing blackouts». *Daily Beast* (12 de junio de 2017). <https://www.thedailybeast.com/newly-discovered-nightmare-cyber-weapon-is-already-causing-blackouts> <<

[10] ZETTER, Kim. «Inside the cunning, unprecedented hack of Ukraine's power grid». *Wired* (3 de marzo de 2016). <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid> <<

[11] FINKLE, Jim. «U.S. firm blames Russian ‘Sandworm’ hackers for Ukraine outage». *Reuters* (7 de enero de 2016). <https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108> <<

[12] C&M News. «Watch how hackers took over a Ukrainian power station». *YouTube* (24 de junio de 2017). <https://www.youtube.com/watch?v=8ThgK1WXUgk> <<

[13] Dragos, Inc. *CRASHOVERRIDE: Analysis of the threat to electric grid operations* (13 de junio de 2017). <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf> <<

[14] Nicholas Weaver comenta. WEAVER, Nicholas. «A cyber-weapon warhead test». *Lawfare* (14 de junio de 2017). <https://www.lawfareblog.com/cyber-weapon-warhead-test> <<

[15] Esta operación se ha llamado Dragonfly. Security Response Attack Investigation Team. «Dragonfly: Western energy sector targeted by sophisticated attack group». Symantec Corporation (20 de octubre de 2017). <https://www.symantec.com/connect/blogs/dragonfly-western-energysector-targeted-sophisticated-attack-group>. PERLROTH, Nicole; SANGER, David. «Cyberattacks put Russian fingers on the switch at power plants, U.S. says». *New York Times* (15 de marzo de 2018). <https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html> <<

[16] MEYER, Christopher. «This teen hacked 150,000 printers to show how the Internet of Things is shit». *Vice Motherboard* (8 de febrero de 2017). <https://motherboard.vice.com/en_us/article/nzqayz/this-teen-hacked-150000-printers-to-show-how-the-internet-of-things-is-shit> <<

[17] STRAUMSHEIM, Carl. «More anti-Semitic fliers printed at universities». *Inside Higher Ed* (27 de enero de 2017). <https://www.insidehighered.com/quicktakes/2017/01/27/more-anti-semiticfliers-printed-universities> <<

[18] KITE-POWELL, Jennifer. «3D printed virus to attack cancer cells». *Forbes* (29 de octubre de 2014). <https://www.forbes.com/sites/jenniferhicks/2014/10/29/3d-printed-virus-to-attack-cancer-cells/#7a8dbddb104b>. COLLINS, Katie. «Meet the biologist hacking 3D printed cancer-fighting viruses». *Wired UK* (16 de octubre de 2014). <https://www.wired.co.uk/article/andrew-hessel-autodesk> <<

[19] University of the Basque Country. «Pacemakers with Internet connection, a not-so-distant goal». *Science Daily* (28 de enero de 2015). <https://www.sciencedaily.com/releases/2015/01/150128113715.htm> <<

[20] MCADAMS, Brooke; RIZVI, Ali. «An overview of insulin pumps and glucose sensors for the generalist». *Journal of Clinical Medicine* 5, núm. 1 (4 de enero de 2016). <http://www.mdpi.com/2077-0383/5/1/5>. VANDERVEEN, Tim. «From smart pumps to intelligent infusion systems: The promise of interoperability». *Patient Safety and Quality Healthcare* (27 de mayo de 2014). <http://psqh.com/may-june-2014/from-smart-pumps-to-intelligent-infusion-systems-the-promise-of-interoperability> <<

[21] BELLUCK, Pam. «First digital pill approved to worries about biomedical 'Big Brother'». *New York Times* (13 de noviembre de 2017). <https://www.nytimes.com/2017/11/13/health/digital-pill-fda.html> <<

[22] BARRETINO, Diego. «Smart contact lenses and eye implants will give doctors medical insights». *IEEE Spectrum* (25 de julio de 2017) <https://spectrum.ieee.org/biomedical/devices/smart-contact-lenses-and-eye-implants-will-give-doctors-medical-insights> <<

[23] BORRELL, Brendan. «Precise devices: Fitness trackers are more accurate than ever». *Consumer Reports* (29 de junio de 2017). <https://www.consumerreports.org/fitness-trackers/precise-devices-fitness-trackers-are-more-accurate-than-ever> <<

[24] CUTHBERTSON, Anthony. «This smart collar turns your pet into a living Tamagotchi». *Newsweek* (12 de abril de 2016). <http://www.newsweek.com/smart-collar-pet-kyon-tamagotchi-gps-dog-446754> <<

[25] WILLIAMS, Owen. «All I want for Christmas is LG's adorable cat toy». *Next Web* (21 de febrero de 2016). <http://thenextweb.com/gadgets/2016/02/21/all-i-want-for-christmas-is-lgs-adorable-cat-toy> <<

[26] Livescribe, Inc. *Livescribe Smartpens* (*URL*). <http://www.livescribe.com/en-us/smartpen> [Consulta 24 abril 2018] <<

[27] GRIGGS, Brandon. «'Smart' toothbrush grades your brushing habits». *CNN* (22 de febrero de 2014). <http://www.cnn.com/2014/01/09/tech/innovation/smart-toothbrush-kolibree>. ACHARYA, Sarmistha. «MWC 2016: Oral-B unveils smart toothbrush that uses mobile camera to help you brush your teeth». *International Business Times* (23 de febrero de 2016). <http://www.ibtimes.co.uk/mwc-2016-oral-b-unveils-smart-toothbrush-that-uses-mobile-camera-help-you-brush-better-1545414> <<

[28] BUDDS, Diana. «A smart coffee cup? It's more useful than it sounds». *Fast Company* (9 de noviembre de 2017). <https://www.fastcodesign.com/90150019/the-perfect-smart-coffee-cup-is-here> <<

[29] LUCKHURST, Phoebe. «Thesesextoysandsmarthook-upapps will make your summer hotter than ever». *Evening Standard* (3 de agosto de 2017). <https://www.standard.co.uk/lifestyle/london-life/these-sex-toys-and-smart-apps-will-make-your-summer-hotter-than-ever-a3603056.html> <<

[30] GIBBS, Samuel. «Privacy fears over ‘smart’ Barbie that can listen to your kids». *Guardian* (13 de marzo de 2015). <https://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel> <<

[31] Stanley. *Smart Measure Pro*. <http://www.stanleytools.com/explore/stanley-mobile-apps/stanley-smart-measure-pro> [Consulta: 24 abril 2018] <<

[32] GLASER, April. «Dig gardening? Plant some connected tech this spring». *Wired* (26 de abril de 2016). <https://www.wired.com/2016/04/connected-gardening-tech-iot> <<

[33] WARSI, Samar. «A motorcycle helmet will call an ambulance and text your family if you have an accident». *Vice Motherboard* (26 de diciembre de 2017). <https://motherboard.vice.com/en_us/article/a37bwp/smart-motorcycle-helmet-helli-will-call-ambulance-skully-pakistan> <<

[34] SNOW, Christopher. «Everyone's buying a smart thermostat; here's how to pick one». USA Today (14 de marzo de 2017). https://www.usatoday.com/story /tech/reviewedcom/2017/03/14/smart-thermostats-are-2017s-hottest-home-gadget heres-how-to-pick-the-right-one-for-you/99125582 <<

[35] HILL, Kashmir; MATTU, Surya. «The house that spied on me». *Gizmodo* (7 de febrero de 2018). <https://gizmodo.com/the-house-that-spied-on-me-1822429852> <<

[36] KENNEDY, Rose. «Want a scale that tells more than your weight? Smart scales are it». *Atlanta Journal-Constitution* (14 de agosto de 2017). <http://www.ajc.com/news/health-med-fit-science/want-scale-that-tells-more-than-your-weight-smart-scales-are/XHpLELYnLgn8cQtBtsay6J> <<

[37] BRADFORD, Alina. «Why smart toilets might actually be worth the upgrade». *CNET* (1 de febrero de 2016). <http://www.cnet.com/how-to/smart-toilets-make-your-bathroom-high-tech> <<

[38] COLON, Alex; TORRES, Timothy. «Thebestsmartlight bulbs of 2017». *PC Magazine* (30 de mayo de 2017). <https://www.pcmag.com/article2/0,2817,2483488,00.asp> <<

[39] KIMAND, Eugene; FARR, Christina. «Amazon is exploring ways to deliver items to your car trunk and the inside of your home». *CNBC* (10 de octubre de 2017). <https://www.cnbc.com/2017/10/10/amazon-is-in-talks-with-phrame-and-is-working-on-a-smart-doorbell.html> <<

[40] GABBATT, Adam. «Don’t lose your snooze: The technology that’s promising a better night’s sleep». *Guardian* (5 de enero de 2017). <https://www.theguardian.com/technology/2017/jan/05/sleep-technology-ces-2017-las-vegas-new-products> <<

[41] HAMBLEN, Matt. «Just what IS a smart city?». *Computerworld* (1 de octubre de 2015). <https://www.computerworld.com/article/2986403/internet-of-things/just-what-is-a-smart-city.html> <<

[42] JOHNSON, Tim. «Smart billboards are checking you out and making judgments». *Miami Herald* (20 de septiembre de 2017). <http://www.miamiherald.com/news/nationworld/national/article174197441.h<<

[43] Las metáforas espaciales no tienen sentido: por eso pongo con mayúsculas *Internet* en este libro, incluso aunque muchos manuales de estilo prefieran la minúscula. Una de las premisas de este libro es que Internet es una única red conectada en la que cada parte afecta a las demás; hay que verlo de este modo para hablar con propiedad sobre seguridad <<

[44] Gartner. «Internet of Things». Gartner IT Glossary. <https://www.gartner.com/it-glossary/internet-of-things> [Consulta 24 abril 2018] <<

[45] Gartner. *Gartner says 8.4 billion connected 'things' will be in use in 2017, up 31 percent from 2016* (7 de febrero de 2017). <https://www.gartner.com/newsroom/id/3598917> <<

[46] DANOVA, Tony. «Morgan Stanley: 75 billion devices will be connected to the Internet of Things by 2020». Business Insider (2 de octubre de 2013). <http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10>. BROWN, Peter «20 billion connected Internet of Things devices in 2017, IHS Markit says». Electronics 360 (25 de enero de 2017). <http://electronics360.globalspec.com/article/8032/20-billion-connected-internet-of-things-devices-in-2017-ihs-markit-says>. BOORSTIN, Julia. «An Internet of Things that will number ten billions». CNBC (1 de febrero de 2016). <https://www.cnbc.com/2016/02/01/an-internet-of-things-that-will-number-ten-billions.html>. Statista. *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)* (2018). <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide> <<

[47] SAWH, Michael. «The best smart clothing: From biometric shirts to contactless payment jackets». *Wareable* (26 de septiembre de 2017). <https://www.wareable.com/smart-clothing/best-smart-clothing> <<

[48] RAPHAEL, J. R. «The ‘smart’ everything trend has officially turned stupid». *Computerworld* (7 de enero de 2016). <http://www.computerworld.com/article/3019713/internet-of-things/smart-everything-trend.html> <<

[49] Es un Internet que piensa: algo que siente, planifica y actúa es la definición clásica de robot. MURPHY, Robin R. (2000), «Robotic paradigms». Introduction to AI Robotics. MIT Press. <https://books.google.com/books/about/?id=RVlnL_X6FrwC> <<

[50] En 2016, intenté llamar a esto *world sized web* (‘web tamaño mundo’), aunque Internet+ es mejor. SCHNEIER, Bruce. «The Internet of Things will be the world’s biggest robot». *Forbes* (2 de febrero de 2016). <https://www.forbes.com/sites/bruceschneier/2016/02/02/the-internet-of-things-will-be-the-worlds-biggest-robot> <<

[51] Incluso el periódico conservador *Economist* publicó un editorial en 2017 apoyando la regulación y las responsabilidades para los dispositivos IoT. Economist. «How to manage the computer-security threat». *Economist* (8 de abril de 2017). <https://www.economist.com/news/leaders/21720279-incentives-software-firms-take-security-seriously-are-too-weak-how-manage> <<

[52] Aunque aquí no tratamos el tema, aquí tenéis otro libro excelente que sí lo hace: KLIMBURG, Alexander. *The Darkening Web: The War for Cyberspace*. Penguin, 2017. <https://books.google.com/books/about/?id=kytBvgAACAAJ> <<

[53] Cambridge Cyber Security Summit. «Transparency, communication and conflict». *CNBC* (4 de octubre de 2017). <https://www.cnbc.com/video/2017/10/09/cambridge-cyber-security-summit-transparency-communication-and-conflict.html> <<

[1] ANUBHAV, Ankit. «IoT thermostat bug allows hackers to turn up the heat». *NewSky Security* (20 de julio de 2017). <https://blog.newskysecurity.com/iot-thermostat-bug-allows-hackers-to-turn-up-the-heat-948e554e5e8b> <<

[2] Un *ransomware* es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de eliminar esa restricción. *(N. del t. extraída de Wikipedia.)* <<

[3] FRANCESCHI-BICCHIERAI, Lorenzo. «Hackers make the first-ever ransomware for smart thermostats». *Vice Motherboard* (7 de agosto de 2016). <https://motherboard.vice.com/en_us/article/aekj9j/internet-of-things-ransomware-smart-thermostat> <<

[4] No, no voy a decirte cuál es mi marca <<

[5] ZETTER, Kim. «Is it possible for passengers to hack commercial aircraft?». *Wired* (26 de mayo de 2015). <http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft>. Dillingham, Gerald L.; Wilshusen, Gregory C.; Barkakati, Nabajyoti. «Air traffic control: FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NextGen». GAO-15-370, US Government Accountability Office (14 de abril de 2015). <http://www.gao.gov/assets/670/669627.pdf> <<

[6] GREENBERG, Andy. «Hackers remotely kill a Jeep on the highway with me in it». *Wired* (21 de julio de 2015). <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>, <https://www.youtube.com/watch?v=MK0SrxBC1xs> (vídeo) <<

[7] ARSENE, Liviu. «Hacking vulnerable medical equipment puts millions at risk». *Information Week* (20 de noviembre de 2014). <http://www.informationweek.com/partner-perspectives/bitdefender/hacking-vulnerable-medical-equipment-puts-millions-at-risk/a/d-id/1319873> <<

[8] HAMBLING, David. «Ships fooled in GPS spoofing attack suggest Russian cyberweapon». *New Scientist* (10 de agosto de 2017). <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon> <<

[9] NEAGLE, Colin. «Smart home hacking is easier than you think». *Network World* (2 de abril de 2015). <http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html> <<

[10] Los bloqueadores de anuncios representan el mayor boicot de consumidores de la historia. Blanchfield, Sean. «The state of the blocked web: 2017 global adblock report». *PageFair* (1 de febrero de 2017). <https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf> <<

[11] MURPHY, Kate. «The ad blocking wars». *New York Times* (20 de febrero de 2016). <https://www.nytimes.com/2016/02/21/opinion/sunday/the-ad-blocking-wars.html> <<

[12] CALAIS GUERRA, Pedro H. *et al*. «Exploring the spam arms race to characterize spam evolution». *Electronic Messaging, Anti-Abuse and Spam Conference (CEAS 2010)* (13-14 de julio de 2010). <https://honeytarg.cert.br/spampots/papers/spampots-ceas10.pdf> <<

[13] Los *skimmers* son dispositivos clonadores de tarjetas electrónicas que se instalan en los cajeros automáticos y en las terminales de los puntos de venta. Cuentan con una ranura falsa que copia la banda magnética de las tarjetas de crédito y débito cuando estas son deslizadas para realizar alguna operación. *(N. del t. extraída de Wikipedia.)* <<

[14] NG, Alfred. «Credit card thieves are getting smarter. You can, too». *CNET* (1 de octubre de 2017). <https://www.cnet.com/news/credit-card-skimmers-thieves-are-getting-smarter-you-can-too> <<

[15] SANCHO , David; Huq, Numaan; Michenzi, Massimiliano. «Cashing in on ATM malware: A comprehensive look at various attack types». *Trend Micro* (2017). <https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf> <<

[1] Citado en Dewdney, A. K. «Computer recreations: Of worms, viruses and core war». *Scientific American* (1 de marzo de 1989). <http://corewar.co.uk/dewdney/1989-03.htm> <<

[2] Rod Beckstrom lo resumió de esta manera: Beckstrom, Rod. *Statement to the London Conference on Cyberspace, Internet Corporation for Assigned Names and Numbers* (ICANN) (2 de noviembre de 2011). <https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf> <<

[3] SCHNEIER, Bruce. «The process of security». *Information Security* (1 de abril de 2000). <https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.htr <<

[4] Mystic, nivel 40. He logrado cazarlos todos en una semana desde agosto de 2017, cuando atrapé a Farfetch’d en Seúl, hasta que liberaron a Mewto en Yokohama, y otra vez desde noviembre de 2017 tras atrapar a mi primer Mewto hasta antes de que liberaran a la tercera generación en diciembre. Viajo mucho y pude atrapar a los Pokémons en sus lugares de origen. Aun así, creo que pasará un tiempo hasta que empiece a atrapar a todos los de la tercera generación regionales <<

[5] A finales de 2017, tuve que reemplazar mi iPhone.como parte del proceso, habilité iCloud e intenté hacer una copia de seguridad de los datos de mi teléfono. No estoy seguro de cómo, pero iCloud logró eliminar veinte años de historial de mi calendario. No sé qué habría hecho si no hubiera tenido una copia de seguridad reciente <<

[6] GRIMES, Roger A. «5 reasons why software bugs still plague us». *CSO* (8 de julio de 2014). <https://www.csoonline.com/article/2608330/security/5-reasons-why-software-bugs-still-plague-us.html>. Heinemeier Hansson, David. «Software has bugs. This is normal». *Signal v. Noise* (7 de marzo de 2016). <https://m.signalvnoise.com/software-has-bugs-this-is-normal-f64761a262ca> <<

[7] En 2002, Bill Gates envió su emblemática memoria de informática digna de confianza a todos sus empleados. Ese mismo año, el desarrollo de Windows se detuvo por completo para que todos los empleados pudieran recibir formación en seguridad. Las primeras herramientas de seguridad del ciclo de vida de desarrollo de seguridad de la compañía aparecieron en 2004. Baxi, Abhishek. «From a Bill Gates memo to an industry practice: The story of Security Development Lifecycle». *Windows Central* (10 de marzo de 2014). <https://www.windowscentral.com/bill-gates-memo-industry-practice-story-security-development-cycle> <<

[8] Para ser sinceros, la empresa ha tenido algunos fallos significativos. Kingsley-Hughes, Adrian. «Apple seems to have forgotten about the whole ‘it just works’ thing». *ZDNet* (19 de diciembre de 2017). <http://www.zdnet.com/article/apple-seems-to-have-forgotten-about-the-whole-it-just-works-thing> <<

[9] National Research Council. «Case study: NASA space shuttle flight control software». *Statistical Software Engineering* , National Academies Press (1996). <https://www.nap.edu/read/5018/chapter/4> <<

[10] WETHERHOLT, Martha. «NASA's approach to software assurance». *Crosstalk* (1 de septiembre de 2015). <http://static1.1.sqspcdn.com/static/f/702523/26502332/1441086732177/2015Wetherholt.pdf> <<

[11] BRIGHT, Peter. «How security flaws work: The buffer overflow». *Ars Technica* (25 de agosto de 2015). <https://arstechnica.com/information-technology/2015/08/how-security-flaws-work-the-buffer-overflow> <<

[12] RESCORLA, Eric. «Is finding security holes a good idea?». *IEEE Security & Privacy* 3, núm. 1 (1 de enero de 2005). <https://dl.acm.org/citation.cfm?id=1048817>. Ozment, Andy; Schechter, Stuart. «Milk or wine: Does software security improve with age?». *Proceedings of the 15th USENIX Security Symposium* (1 de julio de 2006). <https://www.microsoft.com/en-us/research/publication/milk-or-wine-does-software-security-improve-with-age> <<

[13] KELLY, Heather. «The ‘Heart-bleed’ security flaw that affects most of the Internet». *CNN* (9 de abril de 2014). <https://www.cnn.com/2014/04/08/tech/web/heartbleed-openssl/index.html> <<

[14] GREENBERG, Andy. «Triple Meltdown: How so many researchers found a 20-year-old chip flaw at the same time». *Wired* (7 de enero de 2018). <https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery> <<

[15] CLARK, Sandy *et al*. «Familiarity breeds contempt: The honeymoon effect and the role of legacy code in zero-day vulnerabilities». *Proceedings of the 26th Annual Computer Security Applications Conference*. (6-10 de diciembre de 2010). <https://dl.acm.org/citation.cfm?id=1920299> <<

[16] ANDERSON, Nate. «How China swallowed 15 % of 'Net traffic for 18 minutes». *Ars Technica* (17 de noviembre de 2010). <https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes> <<

[17] Algunas redes grandes han añadido características de seguridad, pero el documento que define el BGP especifica lo siguiente: «Las cuestiones de seguridad no se discuten en este documento». Rekhter, Yakov; Li, Tony. «A Border Gateway Protocol 4 (BGP-4)». *Network Working Group*, *Internet Engi-neering Task Force* (Marzo de 1995). <https://tools.ietf.org/html/rfc1771> <<

[18] ARNBAK, Axel; GOLDBERG, Sharon. «Loopholes for circumventing the Constitution: Unrestrained bulk surveil-lance on Americans by collecting network traffic abroad». *Michigan Telecommunications and Technology Law Review* 21, núm. 2 (30 de junio de 2014). <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1204&context=mttlr>. Goldberg, Sharon. «Surveillance without borders: The 'traffic shaping' loophole and why it matters». *Century Foundation* (22 de junio de 2017). <https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters> <<

[19] COWIE, Jim. «The new threat: Targeted Internet traffic misdirection». *Vantage Point* , Oracle + Dyn (19 de noviembre de 2013). <https://dyn.com/blog/mitm-internet-hijacking> <<

[20] COWIE, Jim. «The new threat: Targeted Internet traffic misdirection». *Vantage Point* , Oracle + Dyn (19 de noviembre de 2013). <https://dyn.com/blog/mitm-internet-hijacking> <<

[21] GOODIN, Dan. «Suspicious’eventroutestraffic for big-name sites through Russia». *Ars Technica* (13 de diciembre de 2017). <https://arstechnica.com/information-technology/2017/12/suspicious-event-routes-traffic-for-big-name-sites-through-russia> <<

[22] GOODIN, Dan. «Hijacking huge chunks of the internet: A new How To». *Register* (27 de agosto de 2008). <https://www.theregister.co.uk/2008/08/27/bgp_exploit_revealed> <<

[23] TIMBERG, Craig. «A flaw in the design». *Washington Post* (30 de mayo de 2015). <http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1> <<

[24] CARPENTER, Brian E. (ed.). «Architectural principles of the Internet». *Network Working Group, Internet Engineering Task Force* (Junio de 1996). <https://www.ietf.org/rfc/rfc1958.txt> <<

[25] MOORE, Tyler. «The economics of cybersecurity: Principles and policy options». *International Journal of Critical Infrastructure Protection* (2010). <https://tylermoore.utulsa.edu/ijcip10.pdf> <<

[26] En 2017, el cambio se retrasó de nuevo. Internet Corporation for Assigned Names and Numbers. *KSK rollover postponed* (27 de septiembre de 2017). <https://www.icann.org/news/announcement-2017-09-27-en> <<

[27] JORDON, Michael. «Hacking Canon Pixma printers: Doomed encryption». *Context Information Security* (12 de septiembre de 2014). <https://www.contextis.com/blog/hacking-canon-pixma-printers-doomed-encryption> <<

[28] KINNEY, Ralph. «Will it run Doom? Smart thermostat running classic FPS game Doom». *Zareview* (25 de mayo de 2017). <https://www.zareview.com/will-run-doom-smart-thermostat-running-classic-fps-game-doom> <<

[29] J. J. «The DoomBox». Dashfest (1 de marzo de 2010). <http://www.dashfest.com/?p=113> <<

[30] ORLAND, Kyle. «Denuvo's DRM now being cracked within hours of release». *Ars Technica* (19 de octubre de 2017). <https://arstechnica.com/gaming/2017/10/denuvos-drm-ins-now-being-cracked-within-hours-of-release> <<

[31] SCHOEN, Seth. «Thinking about the term ‘backdoor’». *Electronic Frontier Foundation* (17 de marzo de 2016). <https://www.eff.org/deeplinks/2016/03/thinking-about-term-backdoor> <<

[32] SCHNEIER, Bruce. «Why you should side with Apple, not the FBI, in the San Bernardino iPhone case». *Washington Post* (18 de febrero de 2016). <https://www.washingtonpost.com/posteverything/wp/2016/02/18/why-you-should-side-with-apple-not-the-fbi-in-the-san-bernardino-iphone-case> <<

[33] GOODIN, Dan. «Et tu, Fortinet? Hard-coded password raises new backdoor eavesdropping fears». *Ars Technica* (12 de enero de 2016). <https://arstechnica.com/information-technology/2016/01/et-tu-fortinet-hard-coded-password-raises-new-backdoor-eavesdropping-fears> <<

[34] KOROLOV, Maria. «What is a botnet? And why they aren't going away anytime soon». *CSO* (6 de diciembre de 2017). <https://www.csoonline.com/article/3240364/hacking/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html> <<

[35] Ha sido así desde los inicios de la seguridad en Internet. Este es un fragmento de un periódico de 1979: «Pocos o ninguno de los controles de seguridad del ordenador han impedido a un grupo de expertos acceder fácilmente a la información que buscaban». Básicamente, los atacantes siempre ganan. Schell, Roger R. «Computer security: The Achilles' heel of the electronic Air Force?». *Air University Review* 30, núm. 2 (Enero-febrero de 1979) (reprinted in Air & Space Power Journal, Jan-Feb 2013). <http://insct.syr.edu/wp-content/uploads/2015/05/Schell_Achilles_Heel.pdf> <<

[36] SCHNEIER, Bruce. «A plea for simplicity: You can’t secure what you don’t understand». *Information Security* (19 de noviembre de 1999). <https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.htm <<

[37] MCCANDLESS, David. «How many lines of code does it take?». *Information Is Beautiful* (24 de septiembre de 2015). <http://www.informationisbeautiful.net/visualizations/million-lines-of-code> <<

[38] HAY NEWMAN, Lily. «Hackerlexicon: What is an attack surface?». *Wired* (12 de marzo de 2017). <https://www.wired.com/2017/03/hacker-lexicon-attack-surface> <<

[39] MCMILLAN, Robert. «An unexpected security problem in the cloud». *Wall Street Journal* (17 de septiembre de 2017). <https://www.wsj.com/articles/an-unexpected-security-problem-in-the-cloud-1505700061> <<

[40] KADAVNY, Elena. «Thousands of records exposed in Stanford data breaches». *Palo Alto Online* (1 de diciembre de 2017). <https://www.paloaltoonline.com/news/2017/12/01/thousands-of-records-exposed-in-stanford-data-breaches> <<

[41] GEER, Dan. «Cybersecurity as realpolitik». *Black Hat 2014* (6 de agosto de 2014). <http://geer.tinho.net/geer.blackhat.6viii14.txt> <<

[42] Aparte de esos sistemas sociales, nuestra psicología interna y nuestros valores morales nos impiden asesinar a otros <<

[43] HARRIS, Elizabeth A. *et al*. «A sneaky path into Target customers' wallets». *New York Times* (17 de enero de 2014). <https://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html> <<

[44] CIMPANU, Catalin. «New Mirai botnet slams U.S. college with 54-hour DDoS attack». *Bleeping Computer* (30 de marzo de 2017). <https://www.bleepingcomputer.com/news/security/new-mirai-botnet-slams-us-college-with-54-hour-ddos-attack>. Antonakakis, Manos *et al*. «Understanding the Mirai botnet». *Proceedings of the 26th USENIX Security Symposium* (8 de agosto de 2017). <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf> <<

[45] SCHIFFER, Alex. «How a fish tank helped hack a casino». *Washington Post* (21 de julio de 2017). <https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino> <<

[46] Este ensayo describe cómo se interrelacionan Gmail y Netflix en relación con los correos electrónicos, lo que da como resultado una inseguridad: Fisher, James. «The dots do matter: How to scam a Gmail user». *Jameshfisher.com* (7 de abril de 2018). <https://jameshfisher.com/2018/04/07/the-dots-do-matter-how-to-scam-a-gmail-user.html>. Honan, Mat. «How Apple and Amazon security flaws led to my epic hacking». *Wired* (6 de agosto de 2012). <https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking>.
Honan, Mat. «How I resurrected my digital life after an epic hacking». *Wired* (17 de agosto de 2012). <https://www.wired.com/2012/08/mat-honan-data-recovery> <<

[47] VENDA, Pedro. «Hacking DefCon 23's IoT Village Samsung fridge». *Pen Test Partners* (18 de agosto de 2015). «http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge». LEYDEN, John. «Samsung smart fridge leaves Gmail logins open to attack». *Register* (25 de agosto de 2015). <http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar> <<

[48] MICHALEVSKY, Yan; NAKIBLY, Gabi; BONEH, Dan. «Gyrophone: Recognizing speech from gyroscope signals». *Proceedings of the 23rd USENIX Security Symposium* (20-22 de agosto de 2014). <https://crypto.stanford.edu/gyrophone> <<

[49] GOODIN, Dan. «How Kaspersky AV reportedly was caught helping Russian hackers steal NSA secrets». *Ars Technica* (10 de octubre de 2017). <https://arstechnica.com/information-technology/2017/10/russian-hackers-reportedly-used-kaspersky-av-to-search-for-nsa-secrets> <<

[50] CIMPANU, Catalin. «New Mirai botnet slams U.S. college with 54-hour DDoS attack». *Bleeping Computer* (30 de marzo de 2017). <https://www.bleepingcomputer.com/news/security/new-mirai-botnet-slams-us-college-with-54-hour-ddos-attack> <<

[51] Un *rootkit* es un conjunto de software que permite un acceso de privilegio continuo a un ordenador, pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. *(N. del t. extraída de Wikipedia.)* <<

[52] SEALS, Tara. «Enormous malware as a service infrastructure fuels ransomware epidemic». *Infosecurity Magazine* (18 de mayo de 2016). <https://www.infosecurity-magazine.com/news/enormous-malware-as-a-service> <<

[53] SANKIN, Aaron. «Forget Hacking Team, many other companies sell surveillance tech to repressive regimes». *Daily Dot* (9 de julio de 2015). <https://www.dailydot.com/layer8/hacking-team-competitors> <<

[54] US Department of Justice. *Canadian hacker who conspired with and aided Russian FSB officers pleads guilty* (28 de noviembre de 2017). <https://www.justice.gov/opa/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty> <<

[55] SCHNEIER, Bruce. «Class breaks». *Schneier on Security* (3 de enero de 2017). <https://www.schneier.com/blog/archives/2017/01/class_breaks.html> <<

[56] GOODIN, Dan. «Flaw crippling millions of crypto keys is worse than first disclosed». *Ars Technica* (6 de noviembre de 2017). <https://arstechnica.com/information-technology/2017/11/flaw-crippling-millions-of-crypto-keys-is-worse-than-first-disclosed> <<

[57] US Department of Homeland Security. *National risk estimate: Risks to U.S. critical infrastructure from global positioning system disruptions* (Noviembre de 2012). <https://www.hsdl.org/?abstract&did=739832> <<

[58] GREENBERG, Andy. «Security flaw in common keycard locks exploited in string of hotel room break-ins». *Forbes* (26 de noviembre de 2012). <https://www.forbes.com/sites/andygreenberg/2012/11/26/security-flaw-in-common-keycard-locks-exploited-in-string-of-hotel-room-break-ins> <<

[59] GREENBERG, Andy. «Lock firm Onity starts to shell out for security fixes to hotels' hackable locks». *Forbes* (6 de diciembre de 2012). <https://www.forbes.com/sites/andygreenberg/2012/12/06/lock-firm-onity-starts-to-shell-out-for-security-fixes-to-hotels-hackable-locks>. GREENBERG, Andy. «Hotel lock hack still being used in burglaries months after lock firm's fix». *Forbes* (15 de mayo de 2013). <https://www.forbes.com/sites/andygreenberg/2013/05/15/hotel-lock-hack-still-being-used-in-burglaries-months-after-lock-firms-fix>. GREENBERG, Andy. «The hotel room hacker». *Wired* (1 de agosto de 2017). <https://www.wired.com/2017/08/the-hotel-hacker> <<

[60] DIFFIE, Whitfield; HELLMAN, Martin E. «Exhaustive cryptanalysis of the NBS Data Encryption Standard». *Computer* (1 de junio de 1977). <https://www-ee.stanford.edu/~hellman/publications/27.pdf> <<

[61] SCHNEIER, Bruce. Applied Cryptography, 2ª edición. Wiley, 1995 <<

[62] Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*. O'Reilly & Associates, 1998 <<

[63] PELL, Stephanie K.; SOGHOIAN, Christopher. «Your secret Stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy». *Harvard Journal of Law and Technology* 28, núm. 1 (29 de diciembre de 2014). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678> <<

[64] ZETTER, Kim. «Hacker spoofs cell phone tower to intercept calls». *Wired* (31 de julio de 2010). <https://www.wired.com/2010/07/intercepting-cell-phone-calls> <<

[65] Mi ensayo sobre cómo elegir contraseñas seguras: SCHNEIER, Bruce. *Choosing a secure password*. Boing Boing (25 de febrero de 2014). <https://boingboing.net/2014/02/25/choosing-a-secure-password.html> <<

[66] COPPERSMITH, Don. «The Data Encryption Standard (DES) and its strength against attacks». *IBM Journal of Research and Development* 38, núm. 3 (Mayo de 1994). <http://simson.net/ref/1994/coppersmith94.pdf> <<

[67] BIHAM, Eli; SHAMIR, Adi. «Differential cryptanalysis of DES-like cryptosystems» Journal of Cryptology 4, núm. 1 (1990). <https://link.springer.com/article/10.1007/BF00630563> <<

[1] En 2014, Facebook cambió su lema. MURPHY, Samantha. «Facebook changes its 'Move fast and break things' motto». *Mashable* (30 de abril de 2014). <http://mashable.com/2014/04/30/facebooks-new-mantra-move-fast-with-stability/#ebhnHppqdPq9> <<

[2] SHEPHERD, Stephen A. «How do we define responsible disclosure?». SANS Institute (22 de abril de 2003). <https://www.sans.org/reading-room/whitepapers/threats/define-responsible-disclosure-932> <<

[3] GREENBERG, Andy. «Meet 'Project Zero,' Google's secret team of bug-hunting hackers». *Wired* (16 de julio de 2014). <https://www.wired.com/2014/07/google-project-zero>. Hackett, Robert. «Google's elite hacker SWAT team vs. Everyone». *Fortune* (23 de junio de 2017). <http://fortune.com/2017/06/23/google-project-zero-hacker-swat-team> <<

[4] OZMENT, Andy; SCHECHTER, Stuart. «Milk or wine: Does software security improve with age?». *Proceedings of the 15th USENIX Security Symposium* (1 de julio de 2006). <https://www.microsoft.com/en-us/research/publication/milk-or-wine-does-software-security-improve-with-age> <<

[5] Malwarebytes. *PUP reconsideration information: How do we identify potentially unwanted software?* (4 de octubre de 2017). <https://www.malwarebytes.com/pup>. Hutton, Chris. «12 downloads that sneak unwanted software into your PC». *Tom's Guide* (1 de agosto de 2014). <https://www.tomsguide.com/us/top-downloads-unwanted-software,news-19249.html>. <<

[6] FARIVAR, Cyrus. «Equifax CIO, CSO ‘retire’ in wake of huge security breach». *Ars Technica* (15 de septiembre de 2017). <https://arstechnica.com/tech-policy/2017/09/equifax-cio-cso-retire-in-wake-of-huge-security-breach> <<

[7] LEYDEN, John. «‘Amnesia’ IoT botnet feasts on year-old unpatched vulnerability». *Register* (7 de abril de 2017). <https://www.theregister.co.uk/2017/04/07/amnesia_iot_botnet> <<

[8] PAUL, Fredric. «Fixing, upgrading and patching IoT devices can be a real nightmare». *Network World* (7 de septiembre de 2017). <https://www.networkworld.com/article/3222651/internet-of-things/fixing-upgrading-and-patching-iot-devices-can-be-a-real-nightmare.html> <<

[9] CONSTANTIN, Lucian. «Hard-coded password exposes up to 46.000 video surveillance DVRs to hacking». *PC World* (17 de febrero de 2016). <https://www.pcworld.com/article/3034265/hard-coded-password-exposes-up-to-46000-video-surveillance-dvrs-to-hacking.html> <<

[10] HEFFNER, Craig. «How to hack millions of routers». *DefCon 18* (6 de julio de 2010). <https://www.defcon.org/images/defcon-18/dc-18-presentations/Heffner/DEFCON-18-Heffner-Routers.pdf>. Heffner, Craig. «DEFCON 18: How to hack millions of routers». *YouTube* (5 de octubre de 2010). <http://www.youtube.com/watch?v=stnJiPBIM6o> <<

[11] VALENTINO-DEVRIES, Jennifer. «Rarely patched software bugs in home routers cripple security». *Wall Street Journal* (18 de enero de 2016). <https://www.wsj.com/articles/rarely-patched-software-bugs-in-home-routers-cripple-security-1453136285> <<

[12] MILLS, Elinor. «New DNSChanger Trojan variant targets routers». *CNET* (17 de junio de 2008). <http://news.cnet.com/8301-10784_3-9970972-7.html> <<

[13] CLULEY, GRAHAM. «How millions of DSL modems were hacked in Brazil, to pay for Rio prostitutes». *Naked Security* (1 de octubre de 2012). <http://nakedsecurity.sophos.com/2012/10/01/hacked-routers-brazil-vb2012> <<

[14] GOODIN, Dan. «New Linux worm tar-gets routers, cameras, 'Internet of things' devices». Ars Technica (27 de noviembre de 2013). <http://arstechnica.com/security/2013/11/new-linux-worm-targets-routers-cameras-Internet-of-things-devices> <<

[15] MEYER, ROBINSON. «How a bunch of hacked DVR machines took down Twitter and Reddit». Atlantic (21 de octubre de 2016). <https://www.theatlantic.com/technology/archive/2016/10/how-a-bunch-of-hacked-dvr-machines-took-down-twitter-and-reddit/505073> <<

[16] ANTONAKAKIS, Manos et al. «Understanding the Mirai botnet». Proceedings of the 26th USENIX Security Symposium (8 de agosto de 2017). <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf> <<

[17] GREENBERG, Andy. «After Jeep hack, Chrysler recalls 1.4 m vehicles for bug fix». Wired (24 de julio de 2016). <https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix> <<

[18] GOODIN, Dan. «465k patients told to visit doctor to patch critical pacemaker vulnerability». Ars Technica (30 de agosto de 2017). <https://www.arstechnica.com/information-technology/2017/08/465k-patients-need-a-firmware-update-to-prevent-serious-pacemaker-hacks> <<

[19] LEARY, Kyree. «How to update your Kindle and Kindle Fire devices». Digital Trends (27 de abril de 2017). <https://www.digitaltrends.com/mobile/how-to-update-your-kindle> <<

[20] Flexera Software. Vulnerability Review 2017 (13 de marzo de 2017). <https://www.flexera.com/enterprise/resources/research/vulnerability-review> <<

[21] DOBIE, Alex. «Why you'll never have the latest version of Android». Android Central (16 de septiembre de 2012). <http://www.androidcentral.com/why-you-ll-never-have-latest-version-android> <<

[22] KEIZER, Gregg. «Google: Half of Android devices haven’t been patched in a year or more».computerworld (23 de marzo de 2017). <https://www.computerworld.com/article/3184400/android/google-half-of-android-devices-havent-been-patched-in-a-year-or-more.html> <<

[23] KINGSLET-HUGHES, Adrian. «Apple pulls iOS 8.0.1 update, after killing cell service, Touch ID». ZDNet (24 de septiembre de 2014). <http://www.zdnet.com/article/apple-pulls-ios-8-0-1-update-after-ki lling-cell-service-touch-id> <<

[24] GOODIN, Dan. «Update gone wrong leaves 500 smart locks inoperable». Ars Technica (14 de agosto de 2017). <https://www.arstechnica.com/information-technology/2017/08/500-smart-locks-arent-so-smart-anymore-thanks-to-botched-update> <<

[25] SCHWARTZ, Mathew J. «Microsoft pauses Windows security updates to AMD devices». Data Breach Today (9 de enero de 2018). <https://www.databreachtoday.com/microsoft-pauses-windows-securi ty-updates-to-amd-devices-a-10567> <<

[26] SELTZER, Larry. «Microsoft update blunders going out of control». ZDNet (15 de diciembre de 2014). <http://www.zdnet.com/article/has-microsoft-stopped-testing-their-updates> <<

[27] En la actualidad, Microsoft solo soporta las últimas cuatro versiones de Windows. Microsoft Corporation. Windows lifecycle fact sheet (URL). <https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet> [Consulta 24 abril 2018] <<

[28] BARRETT, Brian. «If you still use Windows XP, prepare for the worst». Wired (14 de junio de 2017). <https://www.wired.com/2017/05/still-use-windows-xp-prepare-worst> <<

[29] PARSONS, Jeff. «This is how many computers are still running Windows XP». Mirror (15 de mayo de 2017). <https://www.mirror.co.uk/tech/how-many-computers-still-running-10425650> <<

[30] SANCHO, David; Huq, Numaan; Michenzi, Massimiliano. «Cashing in on ATM malware: A comprehensive look at various attack types». Trend Micro (2017). <https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf> <<

[31] CIMPANU, Catalin. «Backdoor account found in popular ship satellite communications system». Bleeping Computer (26 de octubre de 2017). <https://www.bleepingcomputer.com/news/security/backdoor-account-found-in-popular-ship-satellite-communications-system> <<

[32] ARMASU, Lucian. «Boeing 757 hacked by DHS in cybersecurity test». Tom's Hardware (13 de noviembre de 2017). <http://www.tomshardware.com/news/boeing-757-remote-hack-test,35911.html> <<

[33] GOODIN, Dan. «465k patients told to visit doctor to patch critical pacemaker vulnerability». Ars Technica (30 de agosto de 2017). <https://arstechnica.com/information-technology/2017/08/465k-patients-need-a-firmware-update-to-prevent-serious-pacemaker-hacks> <<

[34] Electronic Frontier Foundation. US v. ElcomSoft Sklyarov (1 de julio de 2011; last updated 7 de agosto de 2012). <https://www.eff.org/cases/us-v-elcomsoft-sklyarov> <<

[35] LEYDEN, John. «HP invokes DMCA to quash Tru64 bug report». Register (31 de julio de 2002). <https://www.theregister.co.uk/2002/07/31/hp_invokes_dmca_to_quash>. McCullagh, Declan. «HP backs down on copyright warning». CNET (2 de agosto de 2002). <https://www.cnet.com/news/hp-backs-down-on-copyright-warning> <<

[36] Electronic Frontier Foundation. Unintended consequences: Fifteen years under the DMCA (1 de marzo de 2013). <https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca> <<

[37] OSBORNE, Charlie. «US DMCA rules updated to give security experts legal backing to research». ZDNet (31 de octubre de 2016). <http://www.zdnet.com/article/us-dmca-rules-updated-to-give-security-experts-legal-backing-to-research> <<

[38] PALLANTE, Maria A. «Section 1201 rulemaking: Sixth triennial proceeding to determine exemptions to the prohibition on circumvention». United States Copyright Office (Octubre de 2015). <https://www.copyright.gov/1201/2015/registers-recommendation.pdf> <<

[39] ZETTER, Kim. «DefCon: Boston subway officials sue to stop talk on fare card hacks». Wired (9 de septiembre de 2008). <https://www.wired.com/2008/08/injunction-requ> <<

[40] PERKINS, Chris. «Volkswagen suppressed a paper about car hacking for 2 years». Mashable (14 de agosto de 2015). <http://mashable.com/2015/08/14/volkswagen-suppress-car-vulnerability> <<

[41] ZETTER, Kim. «A bizarre twist in the debate over vulnerability disclosures». Wired (11 de septiembre de 2016). <https://www.wired.com/2015/09/fireeye-enrw-injunction-bizarre-twist-in-the-debate-over-vulnerability-disclosures> <<

[42] Electronic Frontier Foundation. EFF lawsuit takes on DMCA section 1201: Research and technology restrictions violate the First Amendment (21 de julio de 2016). <https://www.eff.org/press/releases/eff-law suit-takes-dmca-section-1201-research-and-technology-restrictions-violate> <<

[43] ROYCE, Winston. «Managing the development of large software systems». 1970 WESCON Technical Papers 26 (25-28 de agosto de 1970). <https://books.google.com/books?id=9U1GAQAAIAAJ> <<

[44] Agile Alliance. Agile101. <https://www.agilealliance.org/agile101> [Consulta 24 abril 2018] <<

[45] Se ha trabajado en la integración de la seguridad en las prácticas de desarrollo ágil de software. Information Security Forum (Octubre de 2017). Embedding Security into Agile Development: Ten Principles for Rapid Development (unpublished draft) <<

[1] FLEISHMAN, Glenn. «Cartoon captures spirit of the Internet». *New York Times* (14 de diciembre de 2000). <http://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet> <<

[2] HAFEEZ, Kaamran. «Cartoon: ‘Remember when, on the Internet, nobody knew who you were?’». New Yorker (23 de febrero de 2015). <http://www.kaamranhafeez.com/product/remember-internet-nobody-knew-new-yorker-cartoon> <<

[3] Ahora se llama Grupo de Operaciones de Redes Informáticas <<

[4] JOYCE, Rob. «Disrupting nation state hackers». USENIX Enigma 2016 (28 de enero de 2016). <https://www.youtube.com/watch?v=bDJb8WOJYdA> (vídeo), <https://www.usenix.org/sites/default/files/conference/protected-files/enigma_slides_joyce.pdf> (dispositivas) <<

[5] KOERNER, Brendan I. «Inside the cyberattack that shocked the U.S. government». Wired (23 de octubre de 2016). <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government> <<

[6] KREBS, Brian. «Target hackers broke in via HVAC company». KREBS on Security (5 de febrero de 2014). <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company> <<

[7] FINKLE, Jim. «Iranian hackers use fake Facebook accounts to spy on U.S., others». Reuters (29 de mayo de 2014). <http://www.reuters.com/article/iran-hackers/iranian-hackers-use-fake-facebook-accounts-to-spy-on-u-s-others-idUSL1N0OE2CU20140529> <<

[8] FRANCESCHI-BICCHIERAI, Lorenzo. «The vigilante who hacked Hacking Team explains how he did it». Vice Motherboard (15 de abril de 2016). <https://motherboard.vice.com/en_us/article/3dad3n/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it> <<

[9] SANGER, David E.; CORASANTI, Nick. «D.N.C. says Russian hackers penetrated its files, including dossier on Donald TRUMP». New York Times (14 de junio de 2016). <https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html> <<

[10] CSER, Andras. «The Forrester Wave: Privileged identity management, Q3 2016». Forrester (8 de julio de 2016). <https://www.beyondtrust.com/wp-content/uploads/forrester-wave-for-privilege-identity-mana gement-2016.pdf> <<

[11] THOMAS, Kurt; MOSCICKI, Angelika. «New research: Understanding the root cause of account takeover». Google Security Blog (9 de noviembre de 2017). <https://security.googleblog.com/2017/11/new-research-understanding-root-cause.html> <<

[12] SCHNEIER, Bruce. «The curse of the secret question». Schneier on Security (9 de febrero de 2005). <https://www.schneier.com/essays/archives/2005/02/the_curse_of_the_sec.htr <<

[13] LIPTON, Eric; SANGER, David E.; SHANE, SCOTT «The perfect weapon: How Russian cyberpower invaded the U.S.». New York Times (13 de diciembre de 2016). <https://www.nytimes.com/2016/12/13/us/politics/russia.hack-election-dnd> <<

[14] JOHNSON, Alex. «Massive phishing attack targets Gmail users». NBC News (4 de mayo de 2017). <https://www.nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501> <<

[15] SUBRAMANIAN, Nary. «Biometric authentication». Encyclopedia of Cryptography and Security, Springer (1 de enero de 2011). <https://link-springer-com/content/pdf/10.1007%2F978-1-4419-5906-5_775.pdf> <<

[16] ZUCCHERATO, Robert. «Authentication token». Encyclopedia of Cryptography and Security, Springer (1 de enero de 2011). <https://link-springer-com.ezproxy.cul.columbia.edu/referencework/10.1007%2F978-1-4419-5906-5> <<

[17] RAPHAEL, J. R. «What is two-factor authen-tication (2FA)? How to enable it and why you should». CSO (30 de noviembre de 2017). <https://www.csoonline.com/article/3239144/password-security/what-is-two-factor-authentication-2fa-how-to-enable-it-and-why-you-should.html> <<

[18] GREENBERG, Andy. «So hey you should stop using texts for two-factor authentication». Wired (26 de junio de 2016). <https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication> <<

[19] DENT, Steve. «U.S. carriers partner on a better mobile authentication system». Engadget (8 de septiembre de 2017). <https://www.engadget.com/2017/09/08/mobile-authentication-taskforce-att-verizon-tmobile-sprint> <<

[20] SALICE, Dario. «Google’s strongest security, for those who need it most». Keyword (17 de octubre de 2017). <https://www.blog.google/topics/safety-security/googles-strongest-security-those-who-need-it-most> <<

[21] Aquí hay un ejemplo de 2018: Leswing, Kif. «A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note». Business Insider (16 de enero de 2018). <http://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1> <<

[22] ROBBINS, Gary. «The Internet of Things lets you control the world with a smartphone». San Diego Union Tribune (23 de abril de 2017). <http://www.sandiegouniontribune.com/sd-me-connected-home-20170423-story.html> <<

[23] MELENDEZ, Steven. «How to steal a phone number and everything linked to it». Fast Company (18 de julio de 2017). <https://www.fastcompany.com/40432975/how-to-steal-a-phone-number-and-everything-linked-to-it> <<

[24] PEREKALIN, Alex. «Why two-factor authentication is not enough». Kaspersky Daily (19 de mayo de 2017). <https://www.kaspersky.com/blog/ss7-attack-intercepts-sms/16877>. Popper, Nathaniel. «Identity thieves hijack cell-phone accounts to go after virtual currency». New York Times (21 de agosto de 2017). <https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html> <<

[25] Rapid7. «Man-in-the-middle (MITM) attacks». Rapid7 Fundamentals (9 de agosto de 2017). <https://www.rapid7.com/fundamentals/man-in-the-middle-attacks> <<

[26] Gartner. Reviews for online fraud detection. <https://www.gartner.com/reviews/market/OnlineFraudDetectionSystems> [Consulta 24 abril 2018] <<

[27] KUSHNER, David. «The real story of Stuxnet». IEEE Spectrum (26 de febrero de 2013). <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet> <<

[28] GOODIN, Dan. «Stuxnet-stylecode signing is more widespread than anyone thought». Ars Technica (3 de noviembre de 2017). <https://arstechnica.com/information-technology/2017/11/evasive-code-signed-malware-flourished-before-stuxnet-and-still-does>. KIM, Doowon; K won, Bum Jun; Dumitras, Tudor. «Certified malware: Measuring breaches of trust in the Windows code-signing PKI». ACM Conference on Computer and Communications Security (ACM CCS '17) (1 de noviembre de 2017). <http://www.umiacs.umd.edu/~tdumitra/papers/CCS-2017.pdf> <<

[29] HOLPUCH, Amanda. «Facebook adjusts controversial ‘real name’ policy in wake of criticism». Guardian (15 de diciembre de 2015). <https://www.theguardian.com/us-news/2015/dec/15/facebook-change-controversial-real-name-policy> <<

[30] GRIFFITH, Eric. «How to create an anonymous email account». PC Magazine (3 de diciembre de 2017). <https://www.pcmag.com/article2/0,2817,2476288,00.asp> <<

[31] ANDERSON, Nate; FARIVAR, Cyrus. «How the feds took down the Dread Pirate ROBERTS». Ars Technica (3 de octubre de 2013). <https://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts> <<

[32] COX, Joseph. «How the feds use Photoshop to track down pedophiles». Vice Motherboard (15 de junio de 2016). <https://motherboard.vice.com/en_us/article/8q8594/enhance-enhance-enhance-how-the-feds-use-photoshop-to-track-down-pedophiles>. Kelly, Tom. «Ashbourne Interpol officer's role in paedophile suspect hunt». Heath Chronicle (27 de octubre de 2007). <http://www.meathchronicle.ie/news/roundup/articles/2007/03/11/1025-ashbourne-interpol-officers-role-in-paedophile-suspect-hunt> <<

[33] GOODIN, Dan. «Mastermind behind sophisticated, massive botnet outs himself». Ars Technica (5 de diciembre de 2017). <https://arstechnica.com/tech-policy/2017/12/mastermind-behind-massive-botnet-tracked-down-by-sloppy-opsec> <<

[34] LEYDEN, John. «FBI track alleged Anon from unsanitised busty babe pic». Register (13 de abril de 2012). <https://www.theregister.co.uk/2012/04/13/fbi_track_anon_from_iphone_phot
<<

[35] PANETTA, Leon E. «Remarks by Secretary Panetta on cybersecurity to the Business Executives for National Security, New York City». US Department of Defense (11 de octubre de 2012). <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> <<

[36] GREENBERG, Andy. «Security guru Richard CLARKE, talks cyberwar». Forbes (8 de abril de 2010). <http://www.forbes.com/2010/04/08/cyberwar-obama-korea-technology-security-clarke.html> <<

[37] ZETTER, Kim. «NSA hacker chief explains how to keep him out of your system». Wired (29 de enero de 2016). <https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system> <<

[38] US Department of Justice. U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage (19 de mayo de 2014). <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> <<

[39] APUZZO, Matt; LaFraniere, Sharon. «13 Russians indicted as MUELLER, reveals effort to aid TRUMP campaign». New York Times (16 de febrero de 2018). <https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html> <<

[40] EDWARDS, Benjamin et al. «Strategic aspects of cyberattack, attribution, and blame». Proceedings of the National Academy of Sciences of the United States of America 114, núm. 11 (11 de enero de 2017). <http://www.pnas.org/content/pnas/114/11/2825.full.pdf> <<

[41] DERLEFSEN, William R. Cyber attacks, attribution, and dete rren ce: Three case studies . School of Advanced Military Studies, US Army Command and General STAFF College (23 de mayo de 2015). <http://www.dtic.mil/dtic/tr/fulltext/u2/1001276.pdf>. EDWARDS, Benjamin et al. «Strategic aspects of cyber-attack, attribution, and blame». Proceedings of the National Academy of Sciences of the United States of America 114, núm. 11 (11 de enero de 2017). <http://www.pnas.org/content/114/11/2825.full.pdf>. Tran, Delbert. «The law of attribution». Cyber Conflict Project, Yale University (16 de agosto de 2017). <https://law.yale.edu/system/files/area/center/global/document/2017.05.10_-_law_of_attribution.pdf> <<

[42] SCHNEIER, Bruce. «Comments on the Sony hack». Schneier on Security (11 de diciembre de 2014). <https://www.schneier.com/blog/archives/2014/12/comments_on_the.html> <<

[43] SANGER, David E.; Fackler, Martin. «N.S.A. breached North Korean networks before Sony attack, officials say». New York Times (18 de enero de 2015). <https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html> <<

[44] Cuando Rusia atacó en 2018 los Juegos Olímpicos de Invierno en Corea del Sur, trató de culpar a Corea del Norte. NAKASHIMA, Ellen. «Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say». Washington Post (24 de febrero de 2018). <https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-ko rea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html> <<

[1] Hablaremos de esto en el capítulo 11, pero aquí tienes un ejemplo reciente: FARIVAR, Cyrus. «FBI again calls for magical solution to break into encrypted phones». *Ars Technica* (7 de marzo de 2018). <https://arstechnica.com/tech-policy/2018/03/fbi-again-calls-for-magical-solution-to-break-into-encrypted-phones> <<

[2] ZUBOFF, Shoshana. «Big other: Surveillance capitalism and the prospects of an information civilization». Journal of Information Technology 30 (17 de abril de 2015). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754> <<

[3] TAUBE, Aaron. «Apple wants to use your heart rate and facial expressions to figure out what mood you're in». Business Insider (24 de enero de 2014). <http://www.businessinsider.com/apples-mood-based-ad-targeting-patent-2014-1>. MCSTAY, Andrew. «Now advertising billboards can read your emotions… and that's just the start». Conversation (4 de agosto de 2015). <http://theconversation.com/now-advertising-billboards-can-read-your-emotions-and-thats-just-the-start-45519> <<

[4] MCSTAY, Andrew. «Tech firms want to detect your emotions and expressions, but people don’t like it». Conversation (27 de junio de 2017). <https://theconversation.com/tech-firms-want-to-detect-your-emo tions-and-expressions-but-people-dont-like-it-80153>. Whigham, Nick. «Glitch in digital pizza advert goes viral, shows disturbing future of facial recognition tech». News.com.au (13 de mayo de 2017). <http://www.news.com.au/technology/innovation/design/glitch-in-digital-pizza-advert-goes-viral-shows-disturbing-future-of-facial-recognition-tech/news-story/3b43904b6dd5444a279fd3cd6f8551db> <<

[5] PAUL, Pamela. «Flattery will get an ad nowhere». New York Times (10 de diciembre de 2010). <http://www.nytimes.com/2010/12/12/fashion/12Studied.html> <<

[6] BOUTIN, Paul. «The secretive world of selling data about you». Newsweek (30 de mayo de 2016). <http://www.newsweek.com/secretive-world-selling-data-about-you-464789> <<

[7] COLLINS, Keith. «Google collects Android users' locations even when location services are disabled». Quartz (21 de noviembre de 2017). <https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled>. Mosenia, Arsalan et al. «PinMe: Tracking a smartphone user around the world». IEEE Transactions on Multi-Scale Computing Systems vol. PP, núm. 99 (15 de septiembre de 2017). <http://ieeexplore.ieee.org/document/8038870>. Loran, Christopher. «How you can be tracked even with your GPS turned off». Android Authority (13 de diciembre de 2017). <https://www.androidauthority.com/tracked-gps-off-822865> <<

[8] LIN, Jialiu et al. «Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing». Proceedings of the 2012 International Conference on Ubiquitous Computing, ACM (5-8 de septiembre de 2012). <https://www.winlab.rutgers.edu/janne/privacyasexpectations-ubicomp12-final.pdf> <<

[9] Los vendedores controlan a los clientes utilizando el wifi de sus teléfonos móviles mientras caminan por las tiendas. Clifford, Stephanie; Hardy, Quentin. «Attention, shoppers: Store is tracking your cell». New York Times (14 de julio de 2013). <http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html> <<

[10] MAHESHWARI, Sapna. «That game on your phone may be tracking what you're watching on TV». New York Times (28 de diciembre de 2017). <https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html> <<

[11] Ben Chenand Facebook Corporation. Systems and methods for utilizing wireless communications to suggest connections for a user . US Patent 9.294.991 (22Mar2016). <https://patents.justia.comm/patent/9294991> <<

[12] CRUMP, Catherine et al. You are being tracked: How license plate readers are being used to record Americans' movements. American Civil Liberties Union (17 de julio de 2013). <https://www.aclu.org/files/assets /071613-aclu-alprreport-opt-v05.pdf> <<

[13] CURREN, Dylan. «Are you ready? Here's all the data Facebook and Google have on you». Guardian (30 de marzo de 2018). <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy> <<

[14] Los ajustes, como el modo de incógnito de Chrome o la navegación privada de Firefox, evitan que el navegador guarde tu historial de navegación, aunque no impide que los sitios web que visitas te rastreen <<

[15] GREIMEL, Hans. «Toyotaunveils new self-driving safety tech, targets 2020 autonomous drive». Automotive News (6 de octubre de 2015). <http://www.autonews.com/article/20151006/OEM06/151009894/toyota-unveils-new-self-driving-safety-tech-targets-2020-autonomous> <<

[16] BARTHOLOMEW, Dana. «Long comment regarding a proposed exemption under 17 U.S.C. 1201». Deere and Company (2015). <https://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf> <<

[17] DREDGE, Stuart. «Apple removed drone-strike apps from App Store due to 'objectionable content'». Guardian (30 de septiembre de 2015). <https://www.theguardian.com/technology/2015/sep/30/apple-removing-drone-strikes-app>. FRANCESCHI-BICCHIERAI, Lorenzo. «Apple just banned the app that tracks U.S. drone strikes again». Vice Motherboard (28 de marzo de 2017). <https://motherboard.vice.com/en_us/article/538kan/apple-just-banned-the-app-that-tracks-us-drone-strikes-again> <<

[18] GRIGSBY, Jason. «Apple's policy on satire: 16 apps rejected for 'ridiculing public figures'». Cloudfour (19 de abril de 2010). <https://cloudfour.com/thinks/apples-policy-on-satire-16-rejected-apps> <<

[19] Telegraph Reporters. «Apple removes VPN apps used to evade China's internet censorship». Telegraph (31 de julio de 2017). <http://www.telegraph.co.uk/technology/2017/07/31/apple-removes-vpn-apps-used-evade-chinas-internet-censorship> <<

[20] AdNauseam. AdNauseam banned from the Google Web Store (5 de enero de 2017). <https://adnauseam.io/free-adnauseam.html> <<

[21] SCHNEIER, Bruce. «When it comes to security, we're back to feudalism». Wired (26 de noviembre de 2012). <https://www.wired.com/2012/11/feudal-security> <<

[22] DONATH, Judith. «Uber-FREE: The ultimate advertising experience». Medium (16 de noviembre de 2017). <https://medium.com/@@judithd/the-future-of-self-driving-cars-and-of-advertising-will-be-promoted-rides-free-transportation-b5f7acd702d4> <<

[23] Tras años rechazando permitirles a los consumidores que usaran cápsulas recargables, ahora Keurig les deja usar el café que quieran a cambio de que compren un accesorio especial. Hern, Alex. «Keurig takes steps towards abandoning coffee-pod DRM». Guardian (11 de mayo de 2015). <https://www.theguardian.com/technology/2015/may/11/keurig-takes-steps-towards-abandoning-coffee-pod-drm> <<

[24] BARRET, Brian. «HP has added DRM to its ink cartridges. Not even kidding (updated)». Wired (23 de septiembre de 2016). <https://www.wired.com/2016/09/hp-printer-drm> <<

[25] Electronic Frontier Foundation. Chamberlain Group Inc. v. Skylink Technologies Inc. (last updated 31 de agosto de 2004). <https://www.eff.org/cases/chamberlain-group-inc-v-skylink-technologies-inc>. «Federal Circuit rejects anti-circumvention claim in garage door opener case». Tech Law Journal (31 de agosto de 2004). <http://www.techlawjournal.com/topstories/2004/20040831.asp>. US Supreme Court «Opinion». Lexmark International, Inc. v. Static Control Components, Inc., núm. 12-873 (25 de marzo de 2014). <https://www.supremecourt.gov/opinions/13pdf/12-873_3dq3.pdf> <<

[26] CAMPOS, Hugo. «The heart of the matter». Slate (24 de marzo de 2015). <http://www.slate.com/articles/technology/future_tense/2015/03/patients_shou
<<

[27] MURPH, Darren. «Mileage maniacs hack Toyota's Prius for 116 mpg». Engadget (6 de abril de 2007). <https://www.engadget.com/2007/04/06/mileage-maniacs-hack-toyotas-prius-for-116-mpg> <<

[28] HOAG, Jeremy. «Hack your ride: Cheat codes and workarounds for your car's tech annoyances». Lifehacker (13 de marzo de 2012). <http://lifehacker.com/5893227/hack-your-ride-cheat-codes-and-workarounds-for-your-cars-tech-annoyances> <<

[29] RAFTER, Michelle V. «Decoding what's in your car's black box». Edmunds (22 de julio de 2014). <https://www.edmunds.com/car-technology/car-black-box-recorders-capture-crash-data.html> <<

[30] HALL, Peter. «Car black box data can be used as evidence». Morning Call (7 de junio de 2014). <http://www.mcall.com/mc-car-black-box-data-can-be-used-as-evidence-story.html> <<

[31] HEATON, Brian. «Expert: California car data privacy bill ‘unworkable’». Government Technology (27 de marzo de 2014). <http://www.govtech.com/transportation/Expert-California-Car-Data-Privacy-Bill-Unworkable.html>. <<

[32] KOEBLER, Jason. «Why American farmers are hacking their tractors with Ukrainian firmware». Vice Motherboard (21 de marzo de 2017). <https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware> <<

[33] RADCLIFFE, Jerome. «Hacking medical devices for fun and insulin: Breaking the human SCADA system». Black Hat 2011 (4 de agosto de 2011). <https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf>.
Seegert, Chuck. «Hackers develop DIY remote-monitoring for diabetes». Med Device Online (8 de octubre de 2014). <http://www.meddeviceonline.com/doc/hackers-develop-diy-remote-monitoring-for-diabetes-0001> <<

[34] SCOTT-RAILTON, John et al. «Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware». Citizen Lab (19 de junio de 2017). <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso> <<

[35] SCOTT-RAILTON, John et al. «Reckless redux: Senior Mexican legislators and politicians targeted with NSO spyware». Citizen Lab (29 de junio de 2017). <https://citizenlab.ca/2017/06/more-mexican-nso-targets> <<

[36] SCOTT-RAILTON, John et al. «Reckless III: Investigation into Mexican mass disappearance targeted with NSO spyware». Citizen Lab (10 de julio de 2017). <https://citizenlab.ca/2017/07/mexico-disappearances-nso> <<

[37] SCOTT-RAILTON, John et al. «Reckless IV: Lawyers for murdered Mexican women's families targeted with NSO spyware». Citizen Lab (2 de agosto de 2017). <https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group> <<

[38] SCOTT-RAILTON, John et al. «Reckless V: Director of Mexican anti-corruption group targeted with NSO group's spyware». Citizen Lab (30 de agosto de 2017). <https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption> <<

[39] SCOTT-RAILTON, John et al. «Bitter sweet: Supporters of Mexico's soda tax targeted with NSO exploit links». Citizen Lab (11 de febrero de 2017). <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware> <<

[40] MARCZAK, Bill et al. «Pay no attention to the server behind the proxy: Mapping FinFisher's continuing proliferation». Citizen Lab (15 de octubre de 2015). <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation> <<

[41] GREENWALD, Glenn. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books, 2014. <https://books.google.com/books/?id=AvFzAgAAQBAJ> <<

[42] La cooperación de la industria de las telecomunicaciones es esencial para muchos de los programas de recopilación de la NSA. Eoyang, Mieke. «Beyond privacy and security: The role of the telecommunications industry in electronic surveillance». Aegis Paper Series, núm. 1603, Hoover Institution (6 de abril de 2016). <https://www.hoover.org/research/beyond-privacy-security-role-telecommunications-industry-electronic-surveillance-0> <<

[43] SOLDATOV, Andrei; Borogan, Irina. «Inside the Red Web: Russia's back door onto the internet extract». Guardian (8 de septiembre de 2015). <https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet> <<

[44] SANKIN, Aaron. «Forget Hacking Team. Many other companies s ell surveillance tech to repressive regimes». Daily Dot (9 de julio de 2015). <https://www.dailydot.com/layer8/hacking-team-competitors> <<

[45] O'NEILL, Patrick Howell. «ISS World: The traveling spyware roadshow for dictatorships and democracies». CyberScoop (20 de junio de 2017). <https://www.cyberscoop.com/iss-world-wiretappers-ball-nso-group-ahmed-mansoor> <<

[46] GUERRERO-SAADE, Juan Andres et al. «Penquin's moonlit maze: The dawn of nation-state digital espionage». Kaspersky Lab (Abril de 2017). <https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_PDF_eng.pdf> <<

[47] NORTON-TAYLOR, Richard. «Titan Rain: How Chinese hackers targeted Whitehall». Guardian (4 de septiembre de 2007). <https://www.theguardian.com/technology/2007/sep/04/news.internet> <<

[48] NAKASHIMA, Ellen. «Cyber-intruder sparks response, debate». Washington Post (8 de diciembre de 2011). <https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html> <<

[49] DEWEY, Caitlin. «The U.S. weapons systems that experts say were hacked by the Chinese». Washington Post (28 de mayo de 2013). <https://www.washingtonpost.com/news/worldviews/wp/2013/05/28/the-u-s-weapons-systems-that-experts-say-were-hacked-by-the-chinese> <<

[50] ZETTER, Kim. «Google to stop censoring search results in China after hack attack». Wired (12 de enero de 2010). <https://www.wired.com/2010/01/google-censorship-china> <<

[51] WINDREM, Robert. «China read emails of top U.S. officials». NBC News (10 de agosto de 2015). <https://www.nbcnews.com/news/us-news/china-read-emails-top-us-officials-n406046> <<

[52] KOERNER, Brendan I. «Inside the cyberattack that shocked the U.S. gover nment». Wired (23 de octubre de 2016). <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government>. Perez, Evan. «FBI arrests Chinese national connected to malware used in OPM data breach». CNN (24 de agosto de 2017). <http://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html> <<

[53] Kaspersky Lab Global Research and Analysis Team. «Introducing White Bear». SecureList (30 de agosto de 2017). <https://securelist.com/introducing-whitebear/81638> <<

[54] British Broadcasting Corporation. «Major cyber spy network uncovered». BBC News (29 de marzo de 2009). <http://news.bbc.co.uk/1/hi/world/americas/7970471.stm> <<

[55] Bencsath, Boldizsar et al. Duqu: A Stuxnet-like malware found in the wild. Laboratory of Cryptography and System Security, Budapest University of Technology and Economics (14 de octubre de 2011). <http://www.crysys.hu/publications/files/benc sathPBF11duqu.pdf> <<

[56] NAKASHIMA, Ellen; MILLER, Greg; Tate, Julie. «U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say». Washington Post (19 de junio de 2012). <https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-ir anian-nuclear-efforts-officials-say/2012/06/19/gJQA6 xBPoV_story.html> <<

[57] RASHID, Fahmida Y. «The Mask hack 'beyond anything we've seen so far'». PC Magazine (11 de febrero de 2014). <http://securitywatch.pcmag.com/hacking/320622-the-mask-hack-beyond-anything-we-ve-seen-so-far>. Donohue, Brian. «The Mask: Unveiling the world's most sophisticated APT campaign». Kaspersky Lab Daily (11 de febrero de 2014). <https://www.kaspersky.com/blog/the-mask-unveiling-the-worlds-most-sophisti cated-apt-campaign/3723>. GOODIN, Dan. «Researchers crack open unusually advanced malware that hid for 5 years». Ars Technica (8 de agosto de 2016). <https://arstechnica.com/information-technology/2016/08/researchers-crack-open-unusually-advanced-malware-that-hid-for-5-years> <<

[58] SANG-HUN, Choe. «North Korean hackers stole U.S.-South Korean military plans, lawmaker says». New York Times (10 de octubre de 2017). <https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html> <<

[59] OBAMA, Barack; Jinping, Xi. Remarks by President OBAMA and President Xi of the People's Republic of China in joint press conference. White House Office of the Press Secretary (25 de septiembre de 2015). <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint> <<

[60] MENN, Joseph; FINKLE, Jim. «Chinese economic cyber-espionage plummets in U.S.: Experts». Reuters (20 de junio de 2016). <http://www.reuters.com/article/us-cyber-spying-china/chinese-economic-cyber-espionage-plummets-in-u-s-experts-idUSKCN0Z700D> <<

[61] DAWSEY, Josh; Stephenson, Emily; PETERSON, Andrea. «John Kelly's personal cellphone was compromised, White House believes». Politico (5 de octubre de 2017). <https://www.politico.com/story/2017/10/05/john-kelly-cell-phone-compromised-243514> <<

[62] LEVINE, Mike. «China is ‘leading suspect’ in massive hack of US government networks». ABC News (25 de junio de 2015). <http://abcnews.go.com/US/china-leading-suspect-massive-hack-us-government-networks/story?id=32036222> <<

[63] El presupuesto de la NSA está clasificado, pero se estima en 11.000 millones de dólares. SHANE, SCOTT. «New leaked document outlines U.S. spending on intelligence agencies». New York Times (29 de agosto de 2013). <http://www.nytimes.com/2013/08/30/us/politics/leaked-document-outlines-us-spending-on-intelligence.html>. Holt, Michael. «Top 15 global intelligence agencies with biggest budgets in the world have tripled since 2009-2016». LinkedIn (4 de octubre de 2015). <https://www.linkedin.com/pulse/top-15-global-intelligence-agencies-biggest-budgets-world-holt> <<

[64] EDMUNSON, Anne et al. RAN: Routing around nation-states. Princeton University (10 de marzo de 2017). <https://www.cs.princeton.edu/~jrex/papers/ran17.pdf> <<

[65] DORRER, Kiyo. «Hello, Big Brother: How China controls its citizens through social media». Deutsche Welle (31 de marzo de 2017). <http://www.dw.com/en/hello-big-brother-how-china-controls-its-citizens-through-social-media/a-38243388>. Wang, Maya. «China's dystopian push to revolutionize surveillance». Human Rights Watch (18 de agosto de 2017). <https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance> <<

[66] PAN, Jennifer; ROBERTS, Margaret E. «How censorship in China allows government criticism but silences collective expression». American Political Science Review 107, núm. 2 (Mayo de 2013). <https://gking.harvard.edu/files/censored.pdf> <<

[67] El sistema puede subvertirse, pero combinado con el régimen de vigilancia y cumplimiento de China, y la autocensura resultante, es muy efectivo. Oliver, August. «The Great Firewall: China's misguided —and futile— attempt to control what happens online». Wired (23 de octubre de 2007). <https://www.wired.com/2007/10/ff-chinafirewall> <<

[68] CHIN, Josh; WONG, Gillian. «China's new tool for social control: A credit rating for everything». Wall Street Journal (28 de noviembre de 2016). <https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590> <<

[69] LASAR, Matthew. «Nazi hunt-ing: How France first ‘civilized’ the internet». Ars Technica (22 de junio de 2011). <https://arstechnica.com/tech-policy/2011/06/how-france-proved-that-the-internet-is-not-global>. Faiola, Anthony. «Germany springs to action over hate speech against migrants». Washington Post (6 de enero de 2016). <https://www.washingtonpost.com/world/europe/germany-springs-to-action-over-hate-speech-against-migrants/2016/01/06/6031218e-b315-11e5-8abc-d09392edc612_story.html> <<

[70] CLARKE,, Richard; Knake, Robert K. Cyber War: The Next Threat to National Security and What to Do about It. HARPER COLLINS, 2010. <https://books.google.com/books?id=rNRlR4RGkecC> <<

[71] SANGER, David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown, 2018. <https://books.google.com/books?id=htc7DwAAQBAJ> <<

[72] KAPLAN, Fred. Dark Territory: The Secret History of Cyber War . Simon & Schuster, 2016. <https://books.google.com/books?id=q1AJCgAAQBAJ> <<

[73] Quizá la mejor definición de guerra cibernética esté en el Manual de Tallín . NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2ª edición. Cambridge University Press, 2017. <http://www.cambridge.org/us/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition> <<

[74] KUSHNER, David. The real story of Stuxnet . IEEE Spectrum, 26 de febrero de 2013. <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Langner, Ralph. To kill a centrifuge . Langner Group, 1 de noviembre de 2013. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>. ZETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Crown Books, 2015. <https://books.google.com/books?id=1l2YAwAAQBAJ> <<

[75] A veces se conocen como sistemas SCADA. Hern, Alex. «U.S. power plants ‘vulnerable to hacking’». Guardian (17 de octubre de 2013). <https://www.theguardian.com/technology/2013/oct/17/us-power-plants-hacking>. Wiles, Jack et al. Techno Security’s Guide to Securing SCADA . Ingress, 2008. <https://books.google.com/books?id=sHtIdWn1gnAC> <<

[76] FULGHUM, David A.; Wall, Robert; Barrie, Douglas. «Details about Israel's high-tech strike on Syria». Aviation Week Network (5 de noviembre de 2007). <http://aviationweek.com/awin/details-about-israel-s-high-tech-strike-syria> <<

[77] MARKOFF, John. «Before the gunfire, cyberattacks». New York Times (13 de agosto de 2008). <http://www.nytimes.com/2008/08/13/technology/13cyber.html> <<

[78] CAMPEN, Alan D. (ed.). The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. AFCEA International Press, 1992. <https://archive.org/details/firstinformation00camp> <<

[79] OBAMA, Barack. Statement by the president on progress in the fight against ISIL . White House Office of the Press Secretary (13 de abril de 2016). <https://obamawhitehouse.archives.gov/the-press-office/2016/04/13/statement-president-progress-fight-against-isil> <<

[80] Esta operación se llamó Dragonfly. Security Response Attack Investigation Team. Dragonfly: Western energy sector targeted by sophisticated attack group . Symantec Corporation (20 de octubre de 2017). <https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group> <<

[81] BERGER, Joseph. «A dam, small and unsung, is caught up in an Iranian hacking case». New York Times (25 de marzo de 2016). <http://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html> <<

[82] United States Computer Emergency Readiness Team. Alert (TA17-293ª): Advanced persistent threat activity targeting energy and other critical infrastructure sectors (20 de octubre de 2017). <https://www.us-cert.gov/ncas/alerts/TA17-293A> <<

[83] HERSH, Seymour M. «Preparing the battlefield». New Yorker (7 de julio de 2008). <https://www.newyorker.com/magazine/2008/07/07/preparing-the-battlefield> <<

[84] RUUS, Kertu. «Cyber war I: Estonia attacked from Russia». European Affairs 9, núm. 1-2 (2008). <http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia> <<

[85] ELGIN,, Benjamin; RILEY, Michael. «Now at the Sands Casino: An Iranian hacker in every server». Bloomberg (12 de diciembre de 2014). <http://www.businessweek.com/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas> <<

[86] El nombre que la industria le ha puesto a este tipo de atacante es APT (amenaza persistente avanzada, por sus siglas en inglés) <<

[87] BUCHANAN, Ben. The legend of sophistication in cyber operations. Harvard Kennedy School Belfer Center for Science and International Affairs (Enero de 2017). <https://www.belfercenter.org/publication/legend-sophistication-cyber-operations> <<

[88] DEPACUALE, Scott; Daly, Michael. «The growing threat of cyber mercenaries». Politico (12 de octubre de 2016). <https://www.politico.com/agenda/story/2016/10/the-growing-threat-of-cyber-mercenaries-000221> <<

[89] SANGER, David E.; Kirkpatrick, David D.; PERLROTH,, Nicole. «The world once laughed at North Korean cyberpower. No more». New York Times (15 de octubre de 2017). <https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html> <<

[90] NEGROPONTE, John D. «Annual threat assessment of the Director of National Intelligence». Office of the Director of National Intelligence (11 de enero de 2007). <http://www.au.af.mil/au/awc/awcgate/dni/threat_assessment_11jan07.pdf> <<

[91] BLAIR, Dennis C. Annual threat assessment of the intelligence community for the Senate Select Committee on Intelligence. Office of the Director of National Intelligence (12 de febrero de 2009). <https://www.dni.gov/files/documents/Newsroom/Testimonies/20090212_test <<

[92] BLAIR, Dennis C. Annual threat assessment of the U.S. intelligence community for the Senate Select Committee on Intelligence. Office of the Director of National Intelligence (2 de febrero de 2010). <https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_test <<

[93] COATS, Daniel R. Statement for the record: Worldwide threat assessment of the US intelligence community: Senate Select Committee on Intelligence. Office of the Director of National Intelligence (11 de mayo de 2017). <https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Uncl%20Final.pdf> <<

[94] ILVES, Toomas Hendrik. Rebooting trust? Freedom vs. security in cyberspace. Office of the President, Republic of Estonia (31 de enero de 2014). <https://vp2006-2016.president.ee/en/official-duties/spee ches/9796-qrebooting-trust-freedom-vs-security-in-cyberspaceq> <<

[95] SHEARER, Jarrad. «W32.Stuxnet». Symantec (13 de julio de 2010; updated 26 de septiembre de 2017). <https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99> <<

[96] THOMSON, Iain. «Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide». Register (28 de junio de 2017). <https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware>. Fruhlinger, Josh. «Petya ransomware and NotPetya: What you need to know now». CSO (17 de octubre de 2017). <https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html>. Weaver, Nicholas. «Thoughts on the NotPetya ransomware attack». Lawfare (28 de junio de 2017). <https://lawfareblog.com/thoughts-notpetya-ransomware-attack>. NAKASHIMA, Ellen. «Russian military was behind 'Notpetya' cyberattack in Ukraine, CIA concludes». Washington Post (12 de enero de 2018). <https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html> <<

[97] PERLROTH,, Nicole. «In cyberattack on Saudi firm, U.S. sees Iran firing back». New York Times (23 de octubre de 2012). <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html> <<

[98] SANGER, David E.; Broad, William J. «TRUMP inherits a secret cyberwar against North Korean missiles». New York Times (4 de marzo de 2017). <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html> <<

[99] GALEOTTI, Mark. «The 'Gerasimov Doctrine' and Russian non-linear war». In Moscow's Shadows (6 de julio de 2014). <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war>. Foy, Henry. «Valery Gerasimov, the general with a doctrine for Russia». Financial Times (15 de septiembre de 2017). <https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b> <<

[100] SANGER, David E.; BUMILLER, Elisabeth. «Pentagon to consider cyberattacks acts of war». New York Times (31 de mayo de 2011). <http://www.nytimes.com/2011/06/01/us/politics/01cyber.html> <<

[101] KELLO, Lucas. The Virtual Weapon and International Order. Yale University Press, 2017. <https://yalebooks.yale.edu/book/9780300220230/virtual-weapon-and-international-order> <<

[102] MORELLO, Carol; MILLER, Greg. «U.S. imposes sanctions on N. Korea following attack on Sony». Washington Post (2 de enero de 2015). <https://www.washingtonpost.com/world/national-security/us-imposes-sanctions-on-n-korea-following-attack-on-sony/2015/01/02/3e5423ae-92af-11e4-a900-9960214d4cd7_story.html> <<

[103] GAMBINO, Lauren; SIDDIQUI, Sabrina. «OBAMA expels 35 Russian diplomats in retaliation for US election hacking». Guardian (30 de diciembre de 2016). <https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack> <<

[104] HEALEY, Jason. «The spectrum of national responsibility for cyberattacks». Brown Journal of World Affairs 18, núm. 1 (2011). <https://www.brown.edu/initiatives/journal-world-affairs/sites/brown.edu.initiatives.journal-world-affairs/files/private/articles/18.1_Healey.pdf> <<

[105] SANGER, David E.; Broad, William J. «TRUMP inherits a secret cyberwar against North Korean missiles». New York Times (4 de marzo de 2017). <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html> <<

[106] KOSTYUK, Nadiya; Zhukov, Yuri M. «Invisible digital front: Can cyber attacks shape battlefield events?». Journal of Conflict Resolution (10 de noviembre de 2017). <http://journals.sagepub.com/doi/pdf/10.1177/0022002717737138> <<

[107] AXELROD, Robert; Iliev, Rum. «Timing of cyber conflict». Proceedings of the National Academy of Sciences of the United States of America 111, núm. 4 (28 de enero de 2014). <http://www.pnas.org/content/111/4/1298> <<

[108] DEWEY, Caitlin. «The U.S. weapons systems that experts say were hacked by the Chinese». Washington Post (28 de mayo de 2013). <https://www.washingtonpost.com/news/worldviews/wp/2013/05/28/the-u-s-weapons-systems-that-experts-say-were-hacked-by-the-chinese>. Weisgerber, Marcus. «China's copycat jet raises questions about F-35». Defense One (23 de septiembre de 2015). <http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859>. Ling, Justin. «Man who sold F-35 secrets to China pleads guilty». Vice News (24 de marzo de 2016). <https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty> <<

[109] El Consejo de Relaciones Exteriores está tratando de supervisarlos a todos ellos. SEGAL, Adam. «Tracking state-sponsored cyber operations». Council on Foreign Relations (6 de noviembre de 2017). <https://www.cfr.org/blog/tracking-state-sponsored-cyber-operations> <<

[110] Para ser justos, que el ataque sea más fácil que la defensa no significa que las operaciones ofensivas del ciberespacio sean más fáciles que las defensivas. Slayton, Rebecca. «What is the cyber offense-defense balance? Conceptions, causes, and assessment». International Security 41, núm. 3 (1 de febrero de 2017). <https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00267?journalCode=isec> <<

[111] RACHMAN, Gideon. «Axis of power». New World, BBC Radio 4 (5 de enero de 2017). <http://www.bbc.co.uk/programmes/b086tfbh> <<

[112] Esta frase se le atribuye a mucha gente, pero esta es la referencia más antigua que he encontrado: KAPLAN, Fred. «How the U.S. could respond to Russia's hacking». Slate (12 de diciembre de 2016). <http://www.slate.com/articles/news_and_politics/war_stories/2016/12/the_u_consequences_for_the_future_of.html> <<

[113] OSBORNE, Charlie. «US hospital pays $55,000 to hackers after ransomware attack». ZDNet (17 de enero de 2018). <http://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators> <<

[114] KREBS, Brian. «Ransomware getting more targeted, expensive». KREBS on Security (16 de septiembre de 2016). <https://krebsonsecurity.com/2016/09/ransomware-getting-more-targeted-expensive> <<

[115] Kaspersky Lab. «Story of the year: The ransomware revolution». Kaspersky Security Bulletin 2016 (28 de noviembre de 2016). <https://media.kaspersky.com/en/business-security/kaspersky-story-of-the-year-ransomware-revolution.pdf> <<

[116] Symantec Corporation. Ransomware and businesses 2016 (19 de julio de 2016). <https://www.symantec.com/content/en/us/enterprise/media/security_response Symantec Corporation. Alarming increase in targeted attacks aimed at politically motivated sabotage and subversion (26 de abril de 2017). <https://www.symantec.com/about/newsroom/press-releases/2017/symantec_0426_01> <<

[117] Carbon Black. The ransomware economy (9 de octubre de 2017). <https://cdn.www.carbonblack.com/wp-content/uploads/2017/10/Car bon-Black-Ransomware-Economy-Report-101117.pdf> <<

[118] WEISMAN, Herb. «Ransomware: Now a billion dollar a year crime and growing». NBC News (9 de enero de 2017). <https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646>. Symantec Corporation. Ransomware and businesses 2016 (19 de julio de 2016). <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers /ISTR2016_Ransomware_and_Businesses.pdf> <<

[119] GRAHAM, Luke. «Cybercrime costs the global economy $450 billion: CEO». CNBC (7 de febrero de 2017). <https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html> <<

[120] MORGAN, Steve. «Cybercrime damages expected to cost the world $6 trillion by 2021». CSO (22 de agosto de 2016). <https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html> <<

[121] BLAIR, Dennis C. et al. Update to the IP Commission Report: The theft of American intellectual property: Reassessments of the challenge and United States Policy . National Bureau of Asian Research (22 de febrero de 2017). <http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.
<<

[122] Federal Bureau of Investigation. Businesse-mail compromise: The 3.1 billion dollar scam (14 de junio de 2016). <https://www.ic3.gov/media/2016/160614.aspx>. KREBS, Brian. «FBI: Extortion, CEO fraud among top online fraud complaints in 2016». KREBS on Security (23 de junio de 2016). <https://krebsonsecurity.com/2017/06/fbi-extortion-ceo-fraud-among-top-online-fraud-complaints-in-2016> <<

[123] HARNEY, Kenneth R. «Scary new scam could swipe all your closing money». Chicago Tribune (31 de marzo de 2016). <http://www.chicagotribune.com/classified/realestate/ct-re-0403-kenneth-harney-column-20160331-column.html> <<

[124] KREBS, Brian. «The scrap value of a hacked PC, revisited». KREBS on Security (12 de octubre de 2012). <https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited> <<

[125] GOODIN, Dan. «Cryptocurrency botnets are rendering some companies unable to operate». Ars Technica (2 de febrero de 2018). <https://arstechnica.com/information-technology/2018/02/cryptocurren cy-botnets-generate-millions-but-exact-huge-cost-on-victims> <<

[126] White Ops. The Methbot operation (20 de diciembre de 2016). <https://www.whiteops.com/hubfs/Resources/WO_Methbot_Operation_WP.p
<<

[127] WAINWRIGHT, Rob et al. «European Union serious and organized crime threat assessment: Crime in the age of technology». Europol (15 de marzo de 2017). <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-as sessment-2017> <<

[128] RAPP, Nicolas; Hackett, Robert. «A hacker's tool kit». Fortune (25 de octubre de 2017). <http://fortune.com/2017/10/25/cybercrime-spyware-marketplace>. GOODIN, Dan. «New IoT botnet offers DDoSes of once-unimaginable sizes for $20». Ars Technica (1 de febrero de 2018). <https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20> <<

[129] DENNING, Dorothy. «North Korea's growing criminal cyberthreat». Conversation (20 de febrero de 2018). <https://theconversation.com/north-koreas-growing-criminal-cyberthreat-89423> <<

[130] KIM, Sam. «Inside North Korea's hacker army». Bloomberg (7 de febrero de 2018). <https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army> <<

[131] ZETTER, Kim. «That insane, $81M Bangladesh bank heist? Here's what we know». Wired (17 de junio de 2016). <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know> <<

[132] KREBS, Brian. «Hacked cameras, DVRs powered today's massive internet outage». KREBS on Security (16 de octubre de 2016). <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage> <<

[133] Proofpoint. Your fridge is full of spam: Proof of an IoT-driven attack (16 de enero de 2014). <https://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM>. GOODIN, Dan. «Is your refrigerator really part of a massive spam-sending botnet?». Ars Technica (17 de enero de 2014). <https://arstechnica.com/information-technolo gy/2014/01/is-your-refrigerator-really-part-of-a-massive-spam-sending-botnet> <<

[134] PAGANINI, Pierluigi. The rise of the IoT botnet: Beyond the Mirai bot. InfoSec Institute (12 de abril de 2017). <http://resources.infosecinstitute.com/rise-iot-botnet-beyond-mirai-bot> <<

[135] FORD, Dana. «Cheney's defibrillator was modified to prevent hacking». CNN (24 de agosto de 2013). <http://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html> <<

[136] KRAVETS, David. «Man accused of sending a seizure-inducing tweet charged with cyberstalking». Ars Technica (17 de marzo de 2017). <https://arstechnica.com/tech-policy/2017/03/man-arrested-for-allegedly-sending-newsweek-writer-a-seizure-inducing-tweet> <<

[137] OVERLY, Steve. «What we know about car hacking, the CIA and those WikiLeaks claims». Washington Post (8 de marzo de 2017). <https://www.washingtonpost.com/news/innovations/wp/2017/03/08/what-we-know-about-car-hacking-the-cia-and-those-wikileaks-claims> <<

[138] FRANCESCHI-BICCHIERAI, Lorenzo. «Hackers make the first-ever ransomware for smart thermostats». Vice Motherboard (7 de agosto de 2016). <https://motherboard.vice.com/en_us/article/aekj9j/Internet-of-things-ransomware-smart-thermostat> <<

[139] MORRIS, David Z. «Hackers hijack hotel's smart locks, demand ransom». Fortune (29 de enero de 2017). <http://fortune.com/2017/01/29/hackers-hijack-hotels-smart-locks> <<

[140] BRANDOM, Russell. «UK hospitals hit with massive ransomware attack». Verge (12 de mayo de 2017). <https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomw are-hack-wannacry-bitcoin>. Gla ser, April. «U.S. hospitals have been hit by the global ransomware attack». Recode (27 de junio de 2017). <https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals> <<

[141] CAMPBELL, Denis; Siddique, Haroon. «Operations cancelled as Hunt accused of ignoring cyber-attack warnings». Guardian (15 de mayo de 2017). <https://www.theguardian.com/technology/2017/may/15/warning-of-nhs-cyber-attack-was-not-acted-on-cybersecurity> <<

[142] ITV. NHS cyber attack: Hospitals no longer diverting patients (16 de mayo de 2017). <http://www.itv.com/news/2017-05-16/nhs-cyber-attack-hospitals-no-longer-diverting-patients> <<

[143] GALLAGHER, Sean. «How one rent-a-botnet army of cameras, DVRs caused Internet chaos». Ars Technica (25 de octubre de 2016). <https://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet> <<

[1] GAULT, Mike. «The CIA secret to cybersecurity that no one seems to get». *Wired* (20 de diciembre de 2016). <https://www.wired.com/2015/12/the-cia-secret-to-cybersecurity-that-no-one-seems-to-get> <<

[2] BLISTEIN, Jon. «Hacker pleads guilty to stealing celebrity nude photos». Rolling Stone (15 de marzo de 2016). <https://www.rollingstone.com/movies/news/hacker-pleads-guilty-to-stealing-celebrity-nude-photos-20160315> <<

[3] LORD, Nate. «A timeline of the Ashley Madison hack». Digital Guardian (27 de julio de 2017). <https://digitalguardian.com/blog/timeline-ashley-madison-hack> <<

[4] LIPTON, Eric; SANGER, David E.; SHANE, SCOTT. «The perfect weapon: How Russian cyber-power invaded the U.S.». New York Times (13 de diciembre de 2016). <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html> <<

[5] COWLEY, Stacy. «2.5 million more people potentially exposed in Equifax breach». New York Times (2 de octubre de 2017). <https://www.nytimes.com/2017/10/02/business/equifax-breach.html> <<

[6] KOERNER, Brendan I. «Inside the cyberattack that shocked the U.S. government». Wired (23 de octubre de 2016). <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government>. Perez, Evan. «FBI arrests Chinese national connected to malware used in OPM data breach». CNN (24 de agosto de 2017). <http://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html> <<

[7] Ross Anderson usa este lenguaje en sus escritos. LEVERETT, Eireann; Clayton, Richard; ANDERSON, Ross. Standardization and certification of the 'Internet of Things . Institute for Consumer Policy (6 de junio de 2017). <https://www.conpolicy.de/en/news-detail/standardization-and-certification-of-the-internet-of-things> <<

[8] ZETTER, Kim. «Simulated cyberattack shows hackers blasting away at the power grid». Wired (26 de septiembre de 2007). <https://www.wired.com/2007/09/simulated-cyber> <<

[9] ZETTER, Kim. «A cyberattack has caused confirmed physical damage for the second time ever». Wired (1 de enero de 2015). <https://www.wired.com/2015/01/german-steel-mill-hack-destruction> <<

[10] BERGER, Joseph. «A dam, small and unsung, is caught up in an Iranian hacking case». New York Times (25 de marzo de 2016). <http://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html> <<

[11] PERROW, Charles. Normal Accidents: Living with High-Risk Technologies . Princeton University Press, 1999. <https://www.amazon.com/Normal-Accidents-Living-High-Risk-Technologies/dp/0691004129> <<

[12] MARTINEZ, Michael; NEWSOME, John; MARSH, Rene. «Handgun-firing drone appears legal in video, but FAA, police probe further». CNN (21 de julio de 2015). <http://www.cnn.com/2015/07/21/us/gun-drone-connecticut/index.html> <<

[13] GOLSON, Jordan. «Jeep hackers at it again, this time taking control of steering and braking systems». Verge (2 de agosto de 2016). <https://www.theverge.com/2016/8/2/12353186/car-hack-jeep-cherokee-vulnerability-miller-valasek> <<

[14] ZETTER, Kim. «Hacker can send fatal dose to hospital drug pumps». Wired (8 de junio de 2015). <https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps> <<

[15] ZETTER, Kim. «Is it possible for passengers to hack commer cial aircraft?». Wired (26 de mayo de 2015). <https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft>. Cuth bertson, Anthony. «Hackers expose security flaws with major airlines». Newsweek (20 de diciembre de 2016). <http://www.newsweek.com/hackers-hijack-planes-flight-system-flaw-534071> <<

[16] MORSE, Jack. «Remotely hacking ships shouldn’t be this easy, and yet…». Mashable (18 de julio de 2017). <http://mashable.com/2017/07/18/hacking-boats-is-fun-and-easy> <<

[17] SCHARR, Jill. «Hacking an electronic highway sign is way too easy». Tom's Guide (6 de junio de 2014). <https://www.tomsguide.com/us/highway-signs-easily-hacked,news-18915.html> <<

[18] MCMILLAN, Robert. «Tornado-siren false alarm shows radio-hacking risk». Wall Street Journal (12 de abril de 2017). <https://www.wsj.com/articles/tornado-siren-false-alarm-shows-radio-hacking-risk-1492042082> <<

[19] DENLEY, John. «No nuclear weapon is safe from cyberattacks». Wired (28 de septiembre de 2017). <https://www.wired.co.uk/article/no-nuclear-weapon-is-safe-from-cyberattacks> <<

[20] FALCO, Gregory. The Vacuum of Space Cyber Security. Cyber Security Project, Harvard Kennedy School Belfer Center for Science and International Affairs, unpublished draft (Marzo de 2018) <<

[21] POLLAR, Neal A.; SEGAL, Adam; DeVost, Matthew G. «Trust war: Dangerous trends in cyber conflict». War on the Rocks (16 de enero de 2018). <https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict> <<

[22] MAESE, Rick; BONESTEEL, Matt. «World Anti-Doping Agency report details scope of massive Russian scheme». Washington Post (9 de diciembre de 2016). <https://www.washingtonpost.com/news/early-lead/wp/2016/12/09/wada-report-details-scope-of-massive-rus sian-doping-scheme> <<

[23] DEYOUNG, Karen; NAKASHIMA, Ellen. «UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials». Washington Post (16 de julio de 2016). <https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html> <<

[24] PERLROTH, Nicole; Wines, Michael; Rosenberg, Matthew. «Russian election hacking efforts, wider than previously known, draw little scrutiny». New York Times (1 de septiembre de 2017). <https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html> <<

[25] CLAPPER, James R. Statement for the record: Worldwide threat assessment of the US intelligence community: Senate Armed Services Committee. Office of the Director of National Intelligence (26 de febrero de 2015). <http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf> <<

[26] CARMAN, Ashley. «‘Information integrity’ among top cyber priorities for U.S. gov’t, Clapper says». SC Magazine (11 de septiembre de 2015). <http://www.scmagazine.com/intelligence-committee-hosts-cybersecurity-hearing/article/438202> <<

[27] WILLIAMS, Katie Bo. «Officials worried hackers will change your data, not steal it». Hill (27 de septiembre de 2015). <http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it> <<

[28] CLAPPER, James R. Statement for the record: Worldwide threat assessment of the US intelligence community: Senate Armed Services Committee. Office of the Director of National Intelligence (9 de febrero de 2016). <https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_<<

[29] WATERMAN, Shaun. «Bank regulators briefed on Treasury-led cyber drill». Fed Scoop (20 de julio de 2016). <https://www.fedscoop.com/us-treasury-cybersecurity-drill-july-2016> <<

[30] DEMOS, Telis. «Banks build line of defense for doomsday cyberattack». Wall Street Journal (3 de diciembre de 2017). <https://www.wsj.com/articles/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401> <<

[31] BUCHANAN, Ben; MILLER, Taylor. Machine Learning for Policymakers: What It Is and Why It Matters . Cyber Security Project, Harvard Kennedy School Belfer Center for Science and International Affairs (Junio de 2017). <https://www.belfercenter.org/sites/default/files/files/publication/MachineLea
<<

[32] WONG, Sam. «Google Translate AI invents its own language to translate with». New Scientist (30 de noviembre de 2016). <https://www.newscientist.com/article/2114748-google-translate-ai-invents-its-own-language-to-translate-with>. METZ, Cade. «Facebook's new AI could lead to translations that actually make sense». Wired (9 de mayo de 2017). <https://www.wired.com/2017/05/facebook-open-sources-neural-networks-speed-translations> <<

[33] GIBNEY, Elizabeth. «Google AI algorithm masters ancient game of Go». Nature 529 (17 de enero de 2016). <http://www.nature.com/news/google-ai-algorithm-masters-ancient-game-of-go-1.19234> <<

[34] ESTEVA, Andre et al. «Dermatologist-level classification of skin cancer with deep neural networks». Nature 542 (25 de enero de 2017). <https://www.nature.com/nature/journal/v542/n7639/full/nature21056.html> <<

[35] AANDVIG, Julia et al. «Machine bias». ProPublica (23 de mayo de 2016). <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> <<

[36] HOLLEY, Peter. «Teenage suicide is extremely difficult to predict. That's why some experts are turning to machines for help». Washington Post (26 de septiembre de 2017). <https://www.washingtonpost.com/amphtml/news/innovations/wp/2017/09/25/suicide-is-extremely-difficult-to-predict-thats-why-some-experts-are-turning-to-machines-for-help> <<

[37] Debo decir que hay muchas preguntas acerca de este estudio. Wang, Yilun; Kosinski, Michal. «Deep neural networks are more accurate than humans at detecting sexual orientation from facial images». Open Science Framework (15 de febrero de 2017; last updated 16 de octubre de 2017). <https://osf.io/zn79k> <<

[38] ASHENFELTER, Orley. «Predicting the quality and prices of Bordeaux wine». Economic Journal (29 de mayo de 2008). <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0297.2008.02148.x/abstract> <<

[39] HOFFMAN, Mitchell; Kahn, Lisa; Li, Danielle. «Discretion in hiring». National Bureau of Economic Research (Noviembre de 2015). <https://www.nber.org/papers/w21709.pdf> <<

[40] HIMMELSBACH, Adam. «Punting less can be rewarding, but coaches aren't risking jobs on it». New York Times (18 de agosto de 2012). <http://www.nytimes.com/2012/08/19/sports/football/calculating-footballs-risk-of-not-punting-on-fourth-down.html> <<

[41] ADEE, Sally. «ScammerAIcantailor clickbait to you for phishing attacks». New Scientist (17 de agosto de 2016). <https://www.newscientist.com/article/2101483-scammer-ai-can-tailor-clickbait-to-you-for-phishing-attacks> <<

[42] MIOTTO, Riccardo; Kidd, Brian A.; Dudley, Joel T. «Deep Patient: An unsupervised representation to predict the future of patients from the electronic health records». Scientific Reports, 6, núm. 26094 (17 de mayo de 2016). <https://www.nature.com/articles/srep26094> <<

[43] KNIGHT, Will. «The dark secret at the heart of AI». MIT Technology Review (11 de abril de 2017). <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai> <<

[44] MESSNER, William (ed.). Autonomous Technologies: Applications That Matter . SAE International, 2014. <http://books.sae.org/jpf-auv-004> <<

[45] NGUYEN, Anh; Yosinski, Jason; Clune, Jeff. «Deep neural networks are easily fooled: High confidence predictions for unrecognizable images». Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR ’15) (2 de abril de 2015). <https://arxiv.org/abs/1412.1897> <<

[46] SZGEDY, Christian et al. «Intriguing properties of neural networks». Conference Proceedings: International Conference on Learning Representations (ICLR) 2014 (19 de febrero de 2014). <https://arxiv.org/abs/1312.6199> <<

[47] ILYAS, Andrew et al. Partial information attacks on real-world AI . LabSix (20 de diciembre de 2017). <http://www.labsix.org/partial-information-adversarial-examples> <<

[48] VINCENT, James. «Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day». Verge (24 de marzo de 2016). <https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist> <<

[49] LEE, Timothy B. «Dow Jones posts fake story claiming Google was buying Apple». Ars Technica (10 de octubre de 2017). <https://arstechnica.com/tech-policy/2017/10/dow-jones-posts-fake-story-claiming-google-was-buying-apple> <<

[50] PISANI, Bob. «What caused the flash crash? DFTC, DOJ weigh in». CNBC (21 de abril de 2015). <https://www.cnbc.com/2015/04/21/what-caused-the-flash-crash-cftc-doj-weigh-in.html> <<

[51] LEE, Edmund. «AP Twitter account hacked in market-moving attack». Bloomberg (24 de abril de 2013). <https://www.bloomberg.com/news/articles/201 3-04-23/dow-jones-drops-recovers-after-false-repor-on-ap-twitter-page> <<

[52] DVORSKY, George. «Hackers have already started to weaponize artificial intelligence». Gizmodo (11 de septiembre de 2017). <https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425> <<

[53] METZ, Cade. «DARPA goes full Tron with its grand battle of the hack bots». Wired (6 de julio de 2016). <https://www.wired.com/2016/07/__trashed-19> <<

[54] BRAGA, Matthew. «In the future, we'll leave software bug hunting to the machines». Vice Motherboard (16 de junio de 2016). <https://motherboard.vice.com/en_us/article/mg73a8/cyber-grand-challenge>. METZ, Cade. «Hackers don't have to be human anymore. This bot battle proves it». Wired (5 de agosto de 2016). <https://www.wired.com/2016/08/security-bots-show-hacking-isnt-just-humans> <<

[55] GAUDIN, Sharon. «‘Mayhem’ takes first in DARPA hacking challenge».computerworld (5 de agosto de 2016). <https://www.computerworld.com/article/3104891/security/mayhem-takes-first-in-darpas-all-computer-hacking-challenge.html> <<

[56] TOWNSEND, Kevin. «How machine learning will help attackers». Security Week (29 de noviembre de 2016). <http://www.securityweek.com/how-machine-learning-will-help-attackers> <<

[57] Cylance. Black Hat attendees see AI as double-edged sword (1 de agosto de 2017). <https://www.cylance.com/en_us/blog/black-hat-attendees-see-ai-as-double-edged-sword.html> <<

[58] ALLEN, Greg; CHAN, TANiel. Artificial intelligence and national security. Harvard Kennedy School Belfer Center for Science and International Affairs (13 de julio de 2017). <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSe %20final.pdf> <<

[59] BURGESS, Matt. «Ethical hackers have turned this robot into a stabbing machine». Wired (22 de agosto de 2017). <https://www.wired.co.uk/article/hacked-robots-pepper-nao-alpha-2-stab-screwdriver> <<

[60] BONACI, Tamara et al. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robotics. Ar Xiv 1504.04339v1 (17 de abril de 2015). <https://arxiv.org/pdf/1504.04339v1.pdf>. Storm, Darlene. «Researchers hijack teleoperated surgical robot: Remote surgery hacking threats».computerworld (27 de abril de 2015). <https://www.computerworld.com/article/2914741/cybercrime-hacking/researchers-hijack-teleoperated-surgical-robot-remote-surgery-hacking-threats.html> <<

[61] FOX-BREWSTER, Thomas. «Catastrophe warning: Watch an industrial robot get hacked». Forbes (3 de mayo de 2017). <https://www.forbes.com/sites/thomasbrewster/2017/05/03/researchers-hack-industrial-robot-making-a-drone-rotor> <<

[62] SCHARRE, Paul. Army of None: Autonomous Weapons and the Future of War . W. W. Norton, 2017. <https://books.google.com/books?id=sjMsDwAAQBAJ> <<

[63] ROFF, Heather. «Distinguishing autonomous from automatic weapons». Bulletin of the Atomic Scientists (9 de febrero de 2016). <http://thebulletin.org/autonomous-weapons-civilian-safety-and-regulation-versus-prohibition/distinguishing-autonomous-automatic-weapons> <<

[64] SCHARRE, Paul. Autonomous weapons and operational risk . Center for a New American Security (29 de febrero de 2016). <https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk> <<

[65] SAINATO, Michael. «Stephen Hawking, Elon Musk, and Bill Gates warn about artificial intelligence». Observer (19 de agosto de 2015). <http://observer.com/2015/08/stephen-hawking-elon-musk-and-bill-gates-warn-about-artificial-intelligence> <<

[66] RUSSELL, Stuart et al. An open letter: Research priorities for robust and beneficial artificial intelligence . Future of Life Institute (11 de enero de 2015). <https://futureoflife.org/ai-open-letter> <<

[67] Estos dos ensayos hablan sobre el tema: Chiang, Ted. «Silicon Valley is turning into its own worst fear». BuzzFeed (18 de diciembre de 2017). <https://www.buzzfeed.com/tedchiang/the-real-danger-to-civilization-isnt-ai-its-runaway>. Stross, Charlie. «Dude, you broke the future!». Charlie's Diary (Enero de 2018). <http://www.antipope.org/charlie/blog-static/2018/01/dude-you-broke-the-future.html> <<

[68] BROOKS, Rodney. The seven deadly sins of predicting the future of AI (7 de septiembre de 2017). <http://rodneybrooks.com/the-seven-deadly-sins-of-predicting-the-future-of-ai> <<

[69] GALLAGHER, Sean. «Chinese company installed secret backdoor on hundreds of thousands of phones». Ars Technica (15 de noviembre de 2016). <https://arstechnica.com/information-technology/2016/11/chinese-com pany-installed-secret-backdoor-on-hundreds-of-thousands-of-phones> <<

[70] FARIVAR, Cyrus. «Kaspersky under scrutiny after Bloomberg story claims close links to FSB». Ars Technica (11 de julio de 2017). <https://arstechnica.com/information-technology/2017/07/kaspersky-denies-inappropriate-ties-with-russian-govt-after-bloomberg-story> <<

[71] LARSON, Selena. «The FBI, CIA and NSA say Americans shouldn't use Huawei phones». CNN (14 de febrero de 2018). <http://money.cnn.com/2018/02/14/technology/huawei-intelligence-chiefs/index.html> <<

[72] COHEN, Emily G. Check Point response to Mossad rumor . Firewalls Mailing List, Great Circle Associates (7 de julio de 1997). <http://old.greatcircle.com/firewalls/mhonarc/firewalls.199707/msg00223.htm <<

[73] AANDVIG, Julia et al. «AT&Thelped U.S. spy on Internet on a vast scale». New York Times (15 de agosto de 2015). <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html> <<

[74] WEBER, Arnd et al. Sovereignty in information technology: Security, safety and fair market access by openness and control of the supply chain . Karlsruher Institut für Technologie (22 de marzo de 2018). <http://www.itas.kit.edu/pub/v/2018/weua18a.pdf> <<

[75] BECKER, Georg T. et al. «Stealthy dopant-level hardware Trojans: Extended version». Journal of Cryptographic Engineering 4 (Enero de 2014). <https://link.springer.com/article/10.1007/s13389-013-0068-0> <<

[76] MOZUR, Paul. «New rules in China upset Western tech companies». New York Times (28 de enero de 2015). <https://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html> <<

[77] WHITTAKER, Zack. «U.S. government pushed tech firms to hand over source code». ZDNet (17 de marzo de 2016). <http://www.zdnet.com/article/us-government-pushed-tech-firms-to-hand-over-source-code> <<

[78] LEYDEN, John. «‘We’ve nothing to hide’: Kaspersky Lab offers to open up source code». Register (23 de octubre de 2017). <https://www.theregister.co.uk/2017/10/23/kaspersky_source_code_review> <<

[79] SCHECTMAN, Joel; VOLZ, Dustin; STUBBS, Jack. «HP Enterprise let Russia scrutinize cyberdefense system used by Pentagon». Reuters (2 de octubre de 2017). <https://www.reuters.com/article/us-usa-cyber-russia-hpe-specialreport/special-report-hp-enterprise-let-russia-scrutinize-cyberdefense-system-used-by-pentagon-idUSKCN1C716M> <<

[80] TANto si tuvieron éxito como si no, fue ocultado deliberadamente por el New York Times aduciendo asuntos de seguridad nacional. En mi opinión, sí lo hicieron. SANGER, David E.; PERLROTH,, Nicole. «N.S.A. breached Chinese servers seen as security threat». New York Times (23 de marzo de 2014). <https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html> <<

[81] El único documento que tenemos muestra los dispositivos de interceptación de la NSA vinculados con la empresa Syrian Telecomunications Establishment, a cuya red troncal tuvieron acceso. Chief, Access and Target Development (S3261). «Stealthy techniques can crack some of SIGINT's hardest targets». SID Today (Junio de 2010). <http://www.spiegel.de/media/media-35669.pdf>. GALLAGHER, Sean. «Photos of an NSA 'upgrade' factory show Cisco router getting implant». Ars Technica (14 de mayo de 2014). <https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant> <<

[82] PAULI, Darren. «Cisco posts kit to empty houses to dodge NSA chop shops». Register (18 de marzo de 2015). <https://www.theregister.co.uk/2015/03/18/want_to_dodge_nsa_supply_chain <<

[83] ZETTER, Kim. «Secret code found in Juniper's firewalls shows risk of government backdoors». Wired (19 de diciembre de 2015). <https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors> <<

[84] KIRK, Jeremy. «Backdoor found in D-Link router firmware code». InfoWorld (14 de octubre de 2013). <http://www.infoworld.com/article/2612384/network-router/backdoor-found-in-d-link-router-firmware-code.html> <<

[85] BENITEZ, Gio. «How to protect yourself from downloading fake apps and getting hacked». ABC News (7 de noviembre de 2017). <http://abcnews.go.com/US/protect-downloading-fake-apps-hacked/story?id=50972286> <<

[86] FRANCESCHI-BICCHIERAI, Lorenzo. «More than 1 million people downloaded a fake WhatsApp Android app». Vice Motherboard (3 de noviembre de 2017). <https://motherboard.vice.com/en_us/article/evbakk/fake-whatsapp-android-app-1-million-downloads> <<

[87] CONSTANTIN, Lucian. «Malware-infected CCleaner installer distributed to users via official servers for a month». Vice Motherboard (18 de septiembre de 2017). <https://motherboard.vice.com/en_us/article/a3kgpa/ccleaner-backdoor-malware-hack>. FOX-BREWSTER, Thomas. «Avast: The 2.3M CCleaner hack was a sophisticated assault on the tech industry». Forbes (21 de septiembre de 2017). <https://www.forbes.com/sites/thomasbrewster/2017/09/21/avast-ccleaner-attacks-tar get-tech-industry> <<

[88] GREENBERG, Andy. «The Petya plague exposes the threat of evil software updates». Wired (7 de julio de 2017). <https://www.wired.com/story/petya-plague-automatic-software-updates> <<

[89] GRAZIANO, Joseph. Fake AV software updates are distributing malware . Symantec Corporation (21 de noviembre de 2013). <https://www.symantec.com/connect/blogs/fake-av-software-updates-are-distributing-malware> <<

[90] SHWARTZ, Omer et al. «Shattered trust: When replacement smartphone components attack». Proceedings of the 11th USENIX Workshop on Offensive Technologies (WOOT 17) (14 de agosto de 2017). <https://www.usenix.org/conference/woot17/workshop-program/presentation/shwartz> <<

[91] MURPHY, Mike. «Think twice about buying internet-connected devices off eBay». Quartz (18 de diciembre de 2017). <https://qz.com/1156059/dont-buy-second-hand-internet-connected-iot-devices-from-sites-like-ebay-ebay> <<

[92] MAASHO, Aaron. «China denies report it hacked African Union headquarters». Reuters (29 de enero de 2018). <https://www.reuters.com/article/us-africanunion-summit-china/china-denies-report-it-hacked-african-union-headquarters-idUSKBN1FI2I5> <<

[93] SCIOLINO, Elaine. «The bugged embassy case: What went wrong». New York Times (15 de noviembre de 1988). <http://www.nytimes.com/1988/11/15/world/the-bugged-embassy-case-what-went-wrong.html> <<

[94] BUMILLER, Elisabeth; Shanker, Thom. «Panetta warns of dire threat of cyberattack». New York Times (11 de octubre de 2012). <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html> <<

[95] COATS, Daniel R. Statement for the record: Worldwide threat assessment of the US intelligence community: Senate Select Committee on Intelligence. Office of the Director of National Intelligence (11 de mayo de 2017). <https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Uncl%20Final.pdf> <<

[96] COATS, Daniel R. Statement for the record: Worldwide threat as sessment of the US intelligence community . Office of the Director of Na tional Intelligence (13 de febrero de 2018). <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf> <<

[97] RUFFLE, Simon et al. Business blackout: The insurance implications of a cyber attack on the U.S. power grid. Lloyd's Cambridge Centre for Risk Studies (6 de julio de 2015). <https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout> <<

[98] Un ejemplo de esto es Stephen Paddock. Horton, Alex. «The Las Vegas shooter modified a dozen rifles to shoot like automatic weapons». Washington Post (3 de octubre de 2017). <https://www.washingtonpost.com/news/checkpoint/wp/2017/10/02/video-from-las-ve gas-suggests-automatic-gunfire-heres-what-makes-machine-guns-different> <<

[99] ReprapAlgarve. «DIY3Dprinted assassination drone». YouTube (23 de septiembre de 2016). <https://www.youtube.com/watch?v=N3mdUjT6C5w> <<

[100] GOLDSMITH, Jack; RUSSELL, Stuart. «Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations». Aegis Series Paper, Hoover Working Group on National Security, Technology, and Law (5 de junio de 2018). <https://www.hoover.org/sites/default/files/research/docs/381100534-strengths-become-vulnerabilities.pdf> <<

[101] OBAMA, Barack. Press conference by the president. White House Office of the Press Secretary (16 de diciembre de 2016). <https://obamawhitehouse.archives.gov/the-press-office/2016/12/16/press-confe rence-president> <<

[102] Joseph Nye ha escrito mucho sobre la disuasión en el ciberespacio. NYE, Joseph S. Jr. «Deterrence and dissuasion in cyberspace». International Security 41, núm. 3 (1 de febrero de 2017). <https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266> <<

[103] BOHATY, Rochelle F. H. «Dangerously vulnerable». Chemical & Engineering News (12 de enero de 2008). <http://pubs.acs.org/cen/email/html/cen_87_i02_8702gov2.html> <<

[104] Además, los ataques biológicos y los ciberataques son mucho más difíciles de atribuir que los otros, lo que los hace todavía más espantosos <<

[105] PRY, Peter Vincent. «Electromagnetic pulse: Threat to critical infrastructure». Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, House Committee on Homeland Security (8 de mayo de 2014). <http://docs.house.gov/meetings/HM/HM08/20140508/102200/HHRG-113-HM08-Wstate-PryP-20140508.pdf>. GRAHAM, William R.; PRY, Peter Vincent. North Korea nuclear EMP attack: An existential threat . US House of Representatives Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency Hearing (12 de octubre de 2017). <http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf> <<

[106] El término arma de destrucción masiva se está utilizando para casi todo. El FBI se ha referido a las bombas de olla a presión de los terroristas de la maratón de Londres como armas de destrucción masiva. Federal Bureau of Investigation. Weapons of mass destruction. <http://www.fbi.gov/about-us/investigate/terrorism/wmd/wmd_faqs> [Consulta 24 abril 2018]. Palmer, Brian. «When did IEDs become WMD?». Slate (31 de marzo de 2010). <http://www.slate.com/articles/news_and_politics/explainer/2010/03/when_di <<

[107] COATS, Daniel R. Statement for the record: Worldwide threat assessment of the US intelligence community: Senate Select Committee on Intelligence. Office of the Director of National Intelligence (11 de mayo de 2017). <https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Uncl%20Final.pdf> <<

[108] Suskind . The One Percent Doctrine: Deep inside America’s Pursuit of Its Enemies since 9/11 . Simon & Schuster, 2006. <https://www.amazon.com/dp/B000NY12N2/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1> <<

[109] BARRON, James. «The blackout of 2003». New York Times (15 de agosto de 2003). <http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html> <<

[110] US-CERT National Cyber Awareness System. 2003 CERT Advisories . Carnegie Mellon Software Engineering Institute (Diciembre de 2003). <https://www.cert.org/historical/advisories/CA-2003-20.cfm> <<

[111] BARBER, Paul F. et al. Technical analysis of the August 13, 2003 blackout . North American Electric Reliability Council (13 de julio de 2004). <http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07 U.S. Canada Power System Outage Task Force. Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations (1 de abril de 2004). <https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf> <<

[112] KREBS, Brian. «Who is Anna Senpai, the Mirai worm author?». KREBS on Security (18 de enero de 2017). <https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author> <<

[113] GRAFF,Garrett M. «How a dormroom Minecraft scam brought down the Internet». Wired (13 de diciembre de 2017). <https://www.wi red.com/story/mirai-botnet-minecraft-scam-brought-down-the-inter net> <<

[114] OLSON, Parmy. «The day a computer virus came close to plugging Gulf Oil». Forbes (9 de noviembre de 2012). <https://www.forbes.com/sites/parmyolson/2012/11/09/the-day-a-computer-virus-came-close-to-plugging-gulf-oil> <<

[115] THOMSON, Iain. «NotPetya ransomware attack cost us $300m shipping giant Maersk». Register (16 de agosto de 2017). <https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost 300m_says _shipping_giant_maersk> <<

[116] HOBSON, Elton. «Powerful video warns of the danger of autonomous 'slaughterbot' drone swarms». Global News (24 de noviembre de 2017). <https://globalnews.ca/news/3880186/powerful-video-war ns-of-the-danger-of-autonomous-slaughterbot-drone-swarms> <<

[117] HIPPKE, Michael; Learned, John G. Interstellar communication. IX. Message decontamination is possible (6 de febrero de 2018). ArXiv 1802.02180v1. <https://arxiv.org/pdf/1802.02180.pdf> <<

[118] He escuchado el término BRINE usado como acrónimo para referirse a la biología, robótica, información, nanotecnología y energía. Kadtke, James; Wells II, Linton. Policy challenges of accelerating technological change: Security policy and strategy implications of parallel scientific revolutions . Center for Technology and National Security Policy, National Defense University (4 de septiembre de 2014). <http://ctnsp.dodlive.mil/files/2014/09/DTP106.pdf> <<

[119] RUSSETT, Bruce et al. «Did Americans' expectations of nuclear war reduce their savings?». International Studies Quarterly, 38 (Diciembre de 1994). <http://www.jstor.org/discover/10.2307/2600866?uid=3739256&uid=2&uid=4&sid=21103807505461> <<

[120] BEARDSLEE, William R. «Adolescents and the threat of nuclear war: The evolution of a perspective». Yale Journal of Biology and Medicine 56 (Marzo-abril de 1983). <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2589708/pdf/yjbm00104-0020.pdf> <<

[121] Union of Concerned Scientists. Close calls with nuclear weapons (20 de abril de 2015). <http://www.ucsusa.org/sites/default/files/attach/2015/04/Close%20Calls%20v Future of Life Institute. Accidental nuclear war: A timeline (1 de febrero de 2016). <https://futureoflife.org/background/nuclear-close-calls-a-timeline> <<

[122] SCHWARZ, Benjamin. «The real Cuban missile crisis». Atlantic (1 de enero de 2013). <https://www.theatlantic.com/magazine/archive/2013/01/the-real-cuban-missile-crisis/309190> <<

[123] CHAN, Sewell. «Stanislav Petrov, Soviet officer who helped avert nuclear war». New York Times (18 de septiembre de 2017). <https://www.nytimes.com/2017/09/18/world/europe/stanislav-petrov-nuclear-war-dead.html> <<

[124] GEGGEL, Laura. «The odds of dying». Live Science (9 de febrero de 2016). <https://www.livescience.com/3780-odds-dying.html> <<

[125] Por increíble que parezca hoy en día, tras el 11S la gente creía que habría atentados terroristas de igual magnitud cada pocos meses. Pew Research Center. Apr 18-21 2013, omnibus, final topline, N=1,002 . Pew Research Center (Abril de 2013). <http://www.people-press.org/files/legacy-questionnaires/4-23-13%20topline%20for%20release.pdf> <<

[126] GABBATT, Adam. «Boston Marathon bombing injury toll rises to 264». Guardian (23 de abril de 2013). <http://www.theguardian.com/world/2013/apr/23/boston-marathon-injured-toll-rise> <<

[127] National Safety Council. What are the odds of dying from… <http://www.nsc.org/learn/safety-knowledge/Pages/injury-facts-chart. aspx> (texto, gráfico); <http://injuryfacts.nsc.org/all-injuries/preventable-death-overview/odds-of-dying> (gráfico) [Consulta 24 abril 2018]. Gipson, Kevin; Suchy, Adam. Instability of televisions, furniture, and appliances: Estimated and reported fatalities, 2011 report . Consumer Product Safety Commission (Septiembre de 2011). <https://web.archive.org/web/20111007090947/http://www.cpsc.gov/library/fo ver2011.pdf> <<

[128] MUELLER,, John; Stewart, Mark G. «The terrorism delusion: America's overwrought response to September 11». International Security 37, núm. 1 (1 de julio de 2012). <https://politicalscience.osu.edu/faculty/jmueller/absisfin.pdf> <<

[129] GILBERT, Daniel. «If only gay sex caused global warming». Los Angeles Times (2 de julio de 2006). <http://articles.latimes.com/2006/jul/02/opinion/op-gilbert2>. SCHNEIER, Bruce. «The psychology of security». AfricaCrypt 2008 (13 de junio de 2008). <https://www.schneier.com/academic/archives/2008/01/the_psychology_of_se <<

[130] SCHNEIER, Bruce. «Terrorists don’t do movie plots». Wired (8 de septiembre de 2005). <http://www.wired.com/2005/09/terrorists-dont-do-movie-plots> <<

[131] SCHNEIER, Bruce. «Drawing the wrong lessons from horrific events». CNN (31 de julio de 2012). <http://www.cnn.com/2012/07/31/opinion/schneier-aurora-aftermath/index.html> <<

[132] SCHNEIER, Bruce. <Beyond security theater». New Internationalist (Noviembre de 2009). <https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.htr <<

[1] Statista. «Global spam volume as percentage of total e-mail traffic from January 2014 to September 2017, by month» (Octubre de 2017). <https://www.statista.com/statistics/420391/spam-email-traffic-share> <<

[2] ROBERTSON, Jordan. «E-mail spam goes artisanal». Bloomberg (19 de enero de 2016). <https://www.bloomberg.com/news/articles/2016-01-19/e-mail-spam-goes-artisanal> <<

[3] MURDOCH, Steven J. «Liability for push payment fraud pushed onto the victims». Bentham's Gaze (3 de octubre de 2017). <https://www.benthamsgaze.org/2017/10/03/liability-for-push-payment-fraud-pushed-onto-the-victims>. MURDOCH, Steven J.; ANDERSON, Ross. «Security protocols and evidence: Where many payment systems fail». FC 2014: International Conference on Financial Cryptography and Data Security (9 de noviem bre de 2014). <https://link.springer.com/chapter/10.1007/978-3-662-45472-5_2> <<

[4] JENKINS, Patrick; JONES, Sam. «Bank customers may cover cost of fraud under new UK proposals». Financial Times (25 de mayo de 2016). <https://www.ft.com/content/e335211c-2105-11e6-aa98-db1e01fabc0c> <<

[5] Federal Trade Commission. Lost or stolen credit, ATM, and debit cards (Agosto de 2012). <https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards> <<

[6] SCHNEIER, Bruce. Liars and Outliers: Enabling the Trust That Society Needs to Thrive. Wiley, 2012. <http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html> <<

[7] JAYADEV, Arjun; Bowles, Samuel. «Guard labor». Journal of Development Economics 79, núm. 2 (Abril de 2006). <http://www.sciencedirect.com/science/article/pii /S0304387806000125> <<

[8] Gartner. Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017 (16 de agosto de 2017). <https://www.gartner.com/newsroom/id/3784965> <<

[9] GATLIN, Allison. «Cisco, IBM, Dell M&A brawl may whack Symantec, Palo Alto, Fortinet». Investor's Business Daily (8 de febrero de 2016). <https://www.investors.com/news/technology/cisco-ibm-dell-ma-brawl-whacks-symantec-palo-alto-fortinet> <<

[10] Ponemon Institute. 2017 cost of data breach study (20 de junio de 2017). <http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/Whi <<

[11] Symantec Corporation. 2017 Norton cyber security insights report: Global results (23 de enero de 2018). <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf> <<

[12] Yo fui miembro del comité de dirección de este proyecto de investigación. Dreyer, Paul et al. Estimating the global cost of cyber risk . RAND Corporation (14 de enero de 2018). <https://www.rand.org/pubs/research_reports/RR2299.html> <<

[1] MYRSTAD, Finn Lützow-Holm. «#Toyfail: An analysis of consumer and privacy issues in three internet-connected toys». *Forbrukerrådet* (1 de diciembre de 2016). <https://consumermediallc.les.wordpress.com/2016/12/toyfail_report_desembe <<

[2] OLTERMANN, Philip. «German parents told to destroy doll that can spy on children». Guardian (17 de febrero de 2017). <https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children> <<

[3] GIBBS, Samuel. «Hackers can hijack Wi-Fi Hello Barbie to spy on your children». Guardian (26 de noviembre de 2015). <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children> <<

[4] SIEGELBERNARD, Tara et al. «Equifax says cyberattack may have affected 143 million in the U.S.». New York Times (7 de septiembre de 2017). <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html>. COWLEY, Stacy. «2.5 million more people potentially exposed in Equifax breach». New York Times (2 de octubre de 2017). <https://www.nytimes.com/2017/10/02/business/equifax-breach.html> <<

[5] LENART, Lukasz. «S2-045: Possible remote code execution when performing le upload based on Jakarta Multipart parser». Apache Struts 2 Documentation (9 de marzo de 2017). <https://cwiki.apache.org/conuence/display/WW/S2-045>. GOODIN, Dan. «Critical vulnerability under 'massive' attack imperils high-impact sites». Ars Technica (9 de marzo de 2017). <https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites> <<

[6] GOODIN, Dan. «A series of delays and major errors led to massive Equifax breach». Ars Technica (2 de octubre de 2017). <https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach> <<

[7] FARIVAR, Cyrus. «Equifax CIO, CSO ‘retire’ in wake of huge security breach». Ars Technica (15 de septiembre de 2017). <https://arstechnica.com/tech-policy/2017/09/equifax-cio-cso-retire-in-wake-of-huge-security-breach> <<

[8] SCOTT, James. Equifax: America's incredible insecurity . Institute for Critical Infrastructure Technology (20 de septiembre de 2017). <http://icitech.org/wp-content/uploads/2017/09/ICIT-Analysis-Equi fax-Americas-In-Credible-Insecurity-Part-One.pdf> <<

[9] SCHNEIER, Bruce. Testimony and statement for the record: Hearing on ‘securing consumers’ credit data in the age of digital commerce’ before the Subcommittee on Digital Commerce and Consumer Protection Commit-tee on Energy and Commerce, United States House of Representatives (1 de noviembre de 2017). <http://docs.house.gov/meetings/IF/IF17/20171101/106567/HHRG-115-IF17-Wstate-SchneierB-20171101.pdf> <<

[10] FOX-BREWSTER, Thomas. «A brief history of Equifax security fails». Forbes (8 de septiembre de 2017). <https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history> <<

[11] Este es un ejemplo de lo que quiero decir: Open Web Application Security Project. Security by design principles (last modified 3 de agosto de 2016). <https://www.owasp.org/index.php/Security_by_Design_Principles> <<

[12] ZITTRAIN, Jonathan et al. ‘Don’t Panic’ Meets the Internet of Things: Recommendations for a Responsible Future . Berklett Cybersecurity Project, Berkman Center for Internet and Society at Harvard University, unpublished draft (Febrero de 2018) <<

[13] SCHNEIER, Bruce. «Security and privacy guidelines for the Internet of Things». Schneier on Security (9 de febrero de 2017). <https://www.schneier.com/blog/archives/2017/02/security_and_pr.html> <<

[14] Latanya SWEENEY ha hecho un gran trabajo reidentificando datos anónimos. Aquí hay algunos ejemplos: SWEENEY, Latanya. Research accomplishments of Latanya SWEENEY, Ph.D.: Policy and law: Identiability of de-identified data [Consulta 24 abril 2018]. <http://latanyasweeney.org/work/identifiability.html> <<

[15] No es una creencia compartida por todos. Por ejemplo: Littlejohn Shinder, Debra. «From mainframe to cloud: It’s technology déjà vu all over again». TechTalk (27 de julio de 2016). <https://techtalk.gfi.com/from-mainframe-to-cloud-its-technology-deja-vu-all-over-again> <<

[16] Software and Information Industry Association. «Principles for ethical data use». SIAA Issue Brief (15 de septiembre de 2017). <http://www.siia.net/Portals/0/pdf/Policy/Principles%20for%20Ethical%20Da ver=2017-09-15-130746-523>. Kochi, Erica et al. How to prevent discriminatory outcomes in machine learning. Global Future Council on Human Rights 2016-2018, World Economic Forum (12 de marzo de 2018). <http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Preven Outcomes_in_Machine_Learning.pdf> <<

[17] KNIGHT, Will. «The dark secret at the heart of AI». MIT Technology Review (11 de abril de 2017). <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai> <<

[18] Para saber más sobre algoritmos secretos, recomiendo este libro: Pasquale, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, 2015. <http://www.hup.harvard.edu/catalog.php?isbn=9780674368279> <<

[19] HARDESTY, Larry. «Making computers explain themselves». MIT News (27 de octubre de 2016). <http://news.mit.edu/2016/making-computers-explain-themselves-machine-learning-1028>. Castellanos, Sara; Norton, Steven. «Inside DARPA's push to make artificial intelligence explain itself». Wall Street Journal (10 de agosto de 2017). <https://blogs.wsj.com/cio/2017/08/10/inside-darpas-push-to-make-artificial-intelligence-explain-itself>. Hutson, Matthew. «Q&A: Should artificial intelligence be legally required to explain itself?». Science (31 de mayo de 2017). <http://www.sciencemag.org/news/2017/05/qa-should-artificial-intelligence-be-legally-required-explain-itself> <<

[20] El Reglamento General de Protección de Datos de la UE incluye algún tipo de derecho a la explicación. Los expertos siguen debatiendo sobre la amplitud de dicho derecho. GOODMAN, Bryce; Flaxman, Seth. «European Union regulations on algorithmic decision-making and a 'right to explanation'». 2016 ICML Workshop on Human Interpretability in Machine Learning (28 de junio de 2016). <https://arxiv.org/abs/1606.08813>. Wachter, Sandra; Mittelstadt, Brent; Floridi, Luciano. «Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation». International Data Privacy Law 2017 (24 de enero de 2017). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469> <<

[21] KNIGHT, Will. «The dark secret at the heart of AI». MIT Technology Review (11 de abril de 2017). <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai> <<

[22] KUANG, Cliff. «Can A.I. be taught to explain itself?». New York Times Magazine (21 de noviembre de 2017). <https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html> <<

[23] DIAKOPOULOS, Nicholas et al. «Principles for accountable algorithms and a social impact statement for algorithms». Fairness, Accountability, and Transparency in Machine Learning (17 de noviembre de 2016). <https://www.fatml.org/resources/principles-for-accountable-algorithms> <<

[24] HIRSCH, Tad. «Designing contestability: Interaction design, machine learning, and mental health». 2017 Conference on Designing Interactive Systems (9 de septiembre de 2017). <https://dl.acm.org/citation.cfm?doid=3064663.3064703> <<

[25] SANDVIG, Christian et al. «Auditing algorithms: Research methods for detecting discrimination on Internet platforms». 64th Annual Meeting of the International Communication Association (22 de mayo de 2014). <http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20 Preconference.pdf>. Adler, Philip et al. «Auditing black-box models for indirect influence». 2016 IEEE 16th International Conference on Data Mining (ICDM) (23 de febrero de 2016). <http://ieeexplore.ieee.org/document/7837824> <<

[26] AANDVIG, Julia et al. «Machine bias». ProPublica (23 de mayo de 2016). <https://www.propublica.org/article/machine-bias-risk-assess ments-in-criminal-sentencing> <<

[27] HATHAWAY, Melissa E.; SAVAGE, John E. «Stewardship of cyberspace: Duties for internet service providers». CyberDialogue 2012, University of Toronto (9 de marzo de 2012). <https://www.belfercenter.org/sites/default/files/legacy/files/cyberdialogue2012_hathaway-savage. pdf> <<

[28] ROSENCRANCE, Linda. «3 top ISPs to block access to sources of child porn». *Computerworld* (10 de junio de 2008). <https://www.com puterworld.com/article/2535175/networking/3-top-isps-to-block-ac cess-to-sources-of-child-porn.html> <<

[29] Los ingenieros están trabajando en sistemas de seguridad donde los rúters puedan consultar en una base de datos centralizada y saber cuándo un dispositivo de IoT necesita conectarse y qué información está permitido que envíe y reciba. Se llama descripción de uso del fabricante. El rúter puede restringir la conexión del dispositivo para mejorar la seguridad. No digo que sea la manera adecuada de implementar seguridad, pero es una idea que hay que examinar más a fondo. Lear, Eliot; Droms, Ralph; Romascanu, Dan. Manufacturer Usage Description specification . Internet Engineering Task Force (24 de octubre de 2017). <https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud>. Pritikin, Max et al. Bootstrapping remote secure key infrastructures (BRSKI). Internet Engineering Task Force (30 de octubre de 2017). <https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra> <<

[30] Algunas de las sugerencias de este capítulo se han sacado de este informe: HATHAWAY, Melissa E.; SAVAGE, John E. «Stewardship of cyberspace: Duties for internet service providers». CyberDialogue 2012, University of Toronto (9 de marzo de 2012). <https://www.belfercenter.org/sites/default/files/legacy/files/cyberdialogue201savage.pdf> <<

[31] SCHNEIER, Bruce. «Heartbleed». Schneier on Security (9 de abril de 2014). <https://www.schneier.com/blog/archives/2014/04/heartbleed.html> <<

[32] MUTTON, Paul. «Half a million widely trusted websites vulnerable to Heartbleed bug». Netcraft (8 de abril de 2014). <https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html> <<

[33] GRUBB, Ben. «Man who introduced serious 'Heartbleed' security flaw denies he inserted it deliberately». Sydney Morning Herald (11 de abril de 2014). <http://www.smh.com.au/it-pro/security-it/man-who-introduced-serious-heartbleed-security-flaw-denies-he-inserted-it-deliberately-20140410-zqta1.html>. Hern, Alex. «Heartbleed: Developer who introduced the error regrets 'oversight'». Guardian (11 de abril de 2014). <https://www.theguardian.com/technology/2014/apr/11/heartbleed-developer-error-regrets-oversight> <<

[34] VAUGHAN-NICHOLS, Steven J. «Cash, the Core Infrastructure Initiative, and open source projects». ZDNet (28 de abril de 2014). <http://www.zdnet.com/article/cash-the-core-infrastructure-initiative-and-open-source-projects> <<

[35] MCKENZIE, Alex. «Early sketch of ARPANET's first four nodes». Scientific American (5 de diciembre de 2009). <https://www.scientificamerican.com/gallery/early-sketch-of-arpanets-first-four-nodes> <<

[36] WIJERATNE, Yudhanjaya. «The seven companies that really own the Internet». Icarus Wept (28 de junio de 2016). <http://icaruswept.com/2016/06/28/who-owns-the-internet> <<

[37] GOODIN, Dan. «Hack said to cause fiery pipeline blast could rewrite history of cyberwar». Ars Technica (10 de diciembre de 2014). <https://arstechnica.com/information-technology/2014/12/hack-said-to-cause-fiery-pipeline-blast-could-rewrite-history-of-cyberwar> <<

[38] ROMERO, Simon. «N.S.A. spied on Brazilian oil company, report says». New York Times (9 de septiembre de 2013). <http://www.nytimes.com/2013/09/09/world/americas/nsa-spied-on-brazilian-oil-company-report-says.html> <<

[39] HAMBLING, David. «Ships fooled in GPS spoofing attack suggest Russian cyberweapon». New Scientist (10 de agosto de 2017). <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon> <<

[40] Office of Homeland Security. National strategy for homeland security (15 de julio de 2002). <https://www.hsdl.org/?view&did=856>. Bush, George W. The national strategy for the physical protection of critical infrastructures and key assets. Office of the President of the United States (5 de febrero de 2003). <https://www.hsdl.org/?abstract&did=1041>. Homeland Security Council. National strategy for homeland security (5 de octubre de 2007). <https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf>. Bush, George W. Directive on management of domestic incidents. Office of the Federal Register (28 de febrero de 2003). <https://www.hsdl.org/?view&did=439105>. Bush, George W. Directive on national preparedness. Office of the Federal Register (17 de diciembre de 2003). <https://www.hsdl.org/?view&did=441951> <<

[41] OBAMA, Barack. Directive on critical infrastructure security and resilience. White House Office (12 de febrero de 2013). <https://www.hsdl.org/?view&did=731087> <<

[42] TRUMP, Donald J. National security strategy of the United States of America (Diciembre de 2017). <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> <<

[43] NORDEN,Lawrence; FAMIGHETTI, Christopher. America’s voting machines at risk. Brennan Center for Justice, New York University School of Law (15 de septiembre de 2015). <https://www.brennancenter.org/publication/americas-voting-machines-risk> <<

[44] Office of Homeland Security. National strategy for homeland security (15 de julio de 2002). <https://www.hsdl.org/?view &did=856> <<

[45] Un documento que he encontrado dice que solo el 8 % de toda la infraestructura pública es de propiedad privada, pero genera el 75 % de la potencia del país. Bellavita, Christopher. «85 % of what you know about homeland security is probably wrong». Homeland Security Watch (16 de marzo de 2009). <http://www.hlswatch.com/2009/03/16/85-percent-is-wrong> <<

[46] Midwest Publishing Company. Electric utility industry over view. <http://www.midwestpub.com/electricutility_overview.php> [Consulta 24 abril 2018] <<

[47] Aquí tienes un informe: President’s National Infrastructure Advisory Council. Securing cyber assets: Addressing urgent cyber threats to critical infrastructure (14 de agosto de 2017). <https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf> <<

[48] GREENWALD, Glenn. «The crux of the NSA story in one phrase: ‘Collect it all’». Guardian (15 de julio de 2013). <https://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all> <<

[49] SALTZER, Jerome H.; REED, David P.; CLARK, David D. «End-to-end arguments in system design». ACM Transactions on Computer Systems 2, núm. 4 (1 de noviembre de 1984). <http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf> <<

[50] WU, Tim. «How the FCC's net neutrality plan breaks with 50 years of history». Wired (6 de diciembre de 2017). <https://www.wired.com/story/how-the-fccs-net-neutrality-plan-breaks-with-50-years-of-history> <<

[1] La norma ISO 27001 es un buen ejemplo. International Organization for Standardization. *ISO/IEC 27000 family: Information security management systems*. <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> [Consulta 24 abril 2018] <<

[2] SCHLAG, Pierre J. «Rules and standards». UCLA Law Review, 33 (Diciembre de 1985). <https://lawweb.colorado.edu/profiles/pubpdfs/schlag/schlagUCLALR.pdf>.
Black, Julia. Principles based regulation: Risks, challenges and opportunities. University of Sydney. <http://eprints.lse.ac.uk/62814/1/__lse.ac.uk_storage_LIBRARY_Secondary_
<<

[3] COGLIANESE, Cary. «Performancebased regulation: Concepts and challenges». Bignami, Francesca; Zaring, David (eds.).comparative Law and Regulation: Understanding the Global Regulatory Process. Edward Elgar Publishing, 2016. <http://onlinepubs.trb.org/onlinepubs/PBRLit/Coglianese3.pdf> <<

[4] La ley Gramm-Leach-Bliley sobre instituciones financieras es un buen ejemplo. No especifica qué se debe hacer; en su lugar, indica cómo aproximarse al problema e insiste en que las instituciones afectadas establezcan garantías razonables. El resultado es que esas instituciones son flexibles en el cumplimiento y los organismos reguladores lo son en la aplicación. La desventaja es que razonable a menudo se interpreta como todos los demás lo están haciendo, lo que da como resultado una mentalidad de rebaño difícil de cambiar. Cranor, Lorrie Faith et al. «Are they actually any different? Comparing thousands of financial institutions' privacy practices». Twelfth Workshop on the Economics of Information Security (WEIS 2013) (11 de junio de 2013). <https://www.blaseur.com/papers/financial-final.pdf> <<

[5] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity, version 1.1 draft 2 (revised 5 de diciembre de 2017). <https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf> <<

[6] TRUMP, Donald J. Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure . Office of the President of the United States (11 de mayo de 2017). <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure> <<

[7] MCGHEE, Christina. «DoD turns to FedRAMP and cloud brokering». FCW (21 de mayo de 2014). <https://fcw.com/articles/2014/05/21/drill-down-dod-fedramp-and-cloud-brokering.aspx> <<

[8] RAPAPORT, Michael; Francis, Theo. «Equifax says departing CEO won't get $5.2 million in severance pay». Wall Street Journal (26 de septiembre de 2017). <https://www.wsj.com/articles/equifax-says-departing-ceo-wont-get-5-2-million-in-severance-pay-1506449778>. Lamagna, Maria. «After breach, Equifax CEO leaves with $18 million pension, and possibly more». MarketWatch (26 de septiembre de 2017). <https://www.marketwatch.com/story/equifax-ceo-leaves-with-18-million-pension-and-maybe-more-2017-09-26> <<

[9] CIMPANU, Catalin. «Hack cost Equifax only $87.5 million for now». Bleeping Computer (11 de noviembre de 2017). <https://www.bleepingcomputer.com/news/business/hack-cost-equifax-only-87-5-million-for-now> <<

[10] BOMEY, Nathan. «BP's Deepwater Horizon costs total $62B». USA Today (14 de julio de 2016). <https://www.usatoday.com/story/money/2016/07/14/bp-deepwater-horizon-costs/87087056> <<

[11] KAHNEMAN, Daniel; Tversky, Amos. «Prospect theory: An analysis of decision under risk». Econometrica 47, núm. 2 (Marzo de 1979). <https://www.princeton.edu/~kahneman/docs/Publications/prospect_theory.pd
<<

[12] SCHNEIER, Bruce. «How the human brain buys security». IEEE Security & Privacy (Julio-agosto de 2008). <https://www.schneier.com/essays/archives/2008/07/how_the_human_brain.h
<<

[13] GOODIN, Dan. «A series of delays and major errors led to massive Equifax breach». Ars Technica (2 de octubre de 2017). <https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach> <<

[14] CONDLIFFE, Jamie. «A history of Yahoo hacks». MIT Technology Review (15 de diciembre de 2016). <https://www.technologyreview.com/s/603157/a-history-of-yahoo-hacks> <<

[15] GREENBERG, Andy. «Hack brief: Uber paid off hackers to hide a 57-million user data breach». Wired (21 de noviembre de 2017). <https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach> <<

[16] LANGE, Russell; Burger, Eric W. «Long-term market implications of data breaches, not». Journal of Information Privacy and Security (27 de diciembre de 2017). <http://www.tandfonline.com/doi/full/10.1080/15536548.2017.1394070> <<

[17] CARTER, Ash. The Department of Defense cyber strategy. US Department of Defense (17 de abril de 2015). <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> <<

[18] GREER, John Michael. The Wealth of Nature: Economics as if Survival Mattered. New Society Publishers, 2011. <https://books.google.com/books?id=h3-eVcJImqMC> <<

[19] MCROBERTS, Flynn et al. «The fall of Andersen». Chicago Tribune (1 de septiembre de 2002). <http://www.chicagotribune.com/news/chi-0209010315sep01-story.html> <<

[20] GROSS, Megan. «Volkswagen details what top management knew leading up t o emissions revelations». Ars Technica (3 de marzo de 2016). <http://arstechnica.com/cars/2016/03/volkswagen-says-ceo-was-in-fact-briefed-about-emissions-issues-in-2014>. Ivory, Danielle; Bradsher, Keith. «Regulators investigating 2nd VW computer program on emissions». New York Times (8 de octubre de 2015). <http://www.nytimes.com/2015/10/09/business/international/vw-diesel-emis sions-scan dal-congressional-hearing.html>. Gates, Guilbert et al. «Explaining Volkswagen's emissions scandal». New York Times (8 de octubre de 2015; revised 28 de abril de 2016). <http://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html> <<

[21] SCHWARTZ, Jan; Bryan, Victoria. «VW's Dieselgate bill hits $30 bln after another charge». Reuters (29 de septiembre de 2017). <https://www.reuters.com/article/legal-uk-volkswagen-emissions/vws-dieselga te-bill-hits-30-bln-after-another-charge-idUSKCN1C4271> <<

[22] VLASIC, Bill. «Volkswagen official gets 7-year term in diesel-emissions cheating». New York Times (6 de diciembre de 2017). <https://www.nytimes.com/2017/12/06/business/oliver-schmidt-volkswagen.html> <<

[23] BIANCHI JR., Albert; DAMA, Michelle L.; EHRHARDT, Adrienne S. «Executives and board members could face liability for data breaches». National Law Review (3 de marzo de 2017). <https://www.natlawreview.com/article/executives-and-board-members-could-face-liability-data-breaches>. Crace Jr., Joseph B. «When does data breach liability extend to the boardroom?». Law 360 (3 de abril de 2017). <https://www.law360.com/articles/907786> <<

[24] BURGESS, Matt. «TalkTalk's chief executive Dido Harding has resigned». Wired (1 de febrero de 2017). <https://www.wired.co.uk/article/talktalk-dido-harding-resign-quit> <<

[25] SKINNER, Darren C. «Director responsibilities and liability exposure in the era of Sarbanes-Oxley». Practical Lawyer (1 de junio de 2006). <https://www.apks.com/en/perspectives/publications/2006/06/director-responsibilities-and-liability-exposure> <<

[26] WHITE, Mary Jo; Ceresney, Andrew J. «Individual accountability: Not always accomplished through enforcement». New York Law Journal (19 de mayo de 2017). <http://www.law.com/newyorklawjournal/almID/1202786743746> <<

[27] WOOD, Charles Cresson. «Solving the information security & privacy crisis by expanding the scope of top management personal liability». Journal of Legislation 43, núm. 1 (4 de diciembre de 2016). <http://scholarship.law.nd.edu/jleg/vol43/iss1/5> <<

[28] FERNANDES, Earlence; Jung, Jaeyeon; Prakash, Atul. «Security analysis of emerging smart home applications». 2016 IEEE Symposium on Security and Privacy (18 de agosto de 2016). <http://ieeexplore.ieee.org/document/7546527> <<

[29] SmartThings Inc. Welcome to SmartThings! <https://www.smartthings.com/terms> [Consulta 24 abril 2018] <<

[30] A esto se le ha llamado la gran mentira de Internet. Obar, Jonathan A.; Oeldorf-HIRSCH, Anne. «The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services». 44th Research Conference on Communication, Information and Internet Policy 2016 (TPRC 44) (24 de agosto de 2016). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465> <<

[31] Este derecho ha sido impugnado ante los tribunales y hoy en día hay límites a lo que las empresas pueden hacer respecto a las condiciones de uso y servicio de sus productos. Moringiello, Juliet; Ottaviani, John. «Online contracts: We may modify these at any time, right?». Business Law Today (7 de mayo de 2016). <https://www.americanbar.org/publications/blt/2016/05/07_moringiello.html> <<

[32] SILVER-,GREENBERG, Jessica; Gebeloff, Robert. «Arbitration everywhere, stacking the deck of justice». New York Times (31 de octubre de 2015). <https://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html> <<

[33] CHONG, Jane. «We need strict laws if we want more secure software». New Republic (30 de octubre de 2013). <https://newrepublic.com/article/115402/sad-state-software-liability-law-bad-code-part-4> <<

[34] SHARTON, Brenda R.; Kantrowitz, David S. «Equifax and why it's so hard to sue a company for losing your personal information». Harvard Business Review (22 de septiembre de 2017). <https://hbr.org/2017/09/equifax-and-why-its-so-hard-to-sue-a-company-for-losing-your-personal-information> <<

[35] KESTENBAUM, Janis; ENGRAV, Rebecca; EARL, Erin. «4 takeaways from FTC v. D-Link Systems». Law 360 (6 de octubre de 2017). <https://www.law360.com/cybersecurity-privacy/articles/971473> <<

[36] Federal Trade Commission. In the matter of LabMD, Inc., a corporation: Opinion of the commission, Docket núm. 9357 (29 de julio de 2016). <https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf> <<

[37] NEWMAN, Craig A. «LabMD appeal has privacy world waiting». Lexology (18 de diciembre de 2017). <https://www.lexology.com/library/detail.aspx?g=129a4ea7-cc38-4976-94af-3f09e8e280d0> <<

[38] GREENBERG, Andy. «Hotel lock hack still being used in burglaries months after lock firm's fix». Forbes (15 de mayo de 2013). <https://www.forbes.com/sites/andygreenberg/2013/05/15/hotel-lock-hack-still-being-used-in-burglaries-months-after-lock-firms-fix> <<

[39] TAYLOR, Roger J. Escola v. Coca Cola Bottling Co. of Fresno, S.F. 16951. Supreme Court of California (5 de julio de 1944). <https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1150&context= traynor_opinions> <<

[40] United States Code. «18 U.S. Code §2520. Recovery of civil damages authorized». United States Code, 2006 edición 2006, Supp. 5, Title 18, Crimes and Criminal Procedure (2011). <https://www.gpo.gov/fdsys/search/pagedetails.action?packageId=USCODE-2011-title18&granuleId=USCODE-2011-title18-partI-chap119-sec2520> <<

[41] US Copyright Office. «504. Remedies for infringement: Damages and profits». Copyright Law of the United States (Title 17), Chapter 5: Copyright Notice, Deposit, and Registration (Octubre de 2009). <https://www.copyright.gov/title17/92chap5.html> <<

[42] Este artículo presenta muy bien los argumentos de responsabilidad: Burden, Donna L.; Henry, Hilarie L. «Security software vendors battle against impending strict products liability». Product Liability Committee Newsletter, International Association of Defense Counsel (1 de agosto de 2015). <http://www.iadclaw.org/securedocument.aspx?file=1/19/Product_Liability_August_2015.pdf> <<

[43] REIGEL, Greg et al. «GARA: The General Aviation Revitalization Act of 1994». GlobalAir.com (13 de octubre de 2015). <https://blog.globalair.com/post/GARA-the-General-Aviation-Revitalization-Act-of-1994.aspx> <<

[44] JANOFSKY, Adam. «Insurance grows for cyberattacks». Wall Street Journal (17 de septiembre de 2017). <https://www.wsj.com/articles/insurance-grows-for-cyberattacks-1505700360> <<

[45] CHRISTIANO, Paul. «Liability insurance». Sideways View (17 de febrero de 2018). <https://sideways-view.com/2018/02/17/liability-insurance> <<

[46] MERREY, Paul et al. «Seizing the cyber insurance opportunity». KPMG International (12 de julio de 2017). <https://home.kpmg.com/xx/en/home/insights/2017/06/seizing-the-cyber-insurance-opportunity. html>. US House of Representatives. The role of cyber insurance in risk management. Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security (22 de marzo de 2016). <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg22625/html/CHRG-114hhrg22625.htm> <<

[47] JANOFSKY, Adam. «Cyberinsurers look to measure risk». Wall Street Journal (17 de septiembre de 2017). <https://www.wsj.com/articles/cyberinsurers-look-to-measure-risk-1505700301> <<

[48] Hay bastantes historias horribles sobre la seguridad de los monitores de bebés. Silverman, Craig. «7 creepy baby monitor stories that will terrify all parents». BuzzFeed (24 de julio de 2015). <https://www.buzzfeed.com/craigsilverman/creeps-hack-baby-monitors-and-say-terrifying-thing> <<

[49] FRANZEN, Carl. «How to find a hack-proof baby monitor». Lifehacker (4 de agosto de 2017). <https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985> <<

[50] Amazon.com. VTech DM111 audio baby monitor with up to 1,000 ft of range, 5-level sound indicator, digitized transmission & belt clip. <https://www.amazon.com/VTech-DM111-Indicator-Digitized-Transmission/dp/B00JEV5UI8/ref=pd_lpo_vtph_75_bs_lp_t_1> [Consulta 24 abril 2018] <<

[51] He encontrado una evaluación de seguridad de varias marcas: Stanislav, Mark; Beardsley, Tod. «Hacking IoT: A case study on baby monitor exposure and vulnerabilities». Rapid7 (29 de septiembre de 2015). <https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf> <<

[52] AKERLOF, George A. «The market for ‘lemons’: Quality uncertainty and the market mechanism». Quarterly Journal of Economics 84, núm. 3 (1 de agosto de 1970). <https://academic.oup.com/qje/article-abstract/84/3/488/1896241> <<

[53] SCHNEIER, Bruce. «How security companies sucker us with lemons». Wired (19 de abril de 2007). <https://www.wired.com/2007/04/securitymatters-0419> <<

[54] Un estudio estimó que los consumidores tardarían de media 244 horas al año en leer todas las políticas de privacidad que aceptan. McDonald, Aleecia M.; Cranor, Lorrie Faith. «The cost of reading privacy policies». I/S: A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review issue (1 de octubre de 2008). <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf> <<

[55] Samsung. Samsung local privacy policy SmartTV supplement <http://www.samsung.com/hk_en/info/privacy/smarttv> [Consulta 24 abril 2018] <<

[56] GIBBS, Samuel. «Smart fridges and TVs should carry security rating, police chief says». Guardian (24 de julio de 2017). <https://www.theguardian.com/technology/2017/jul/24/smart-tvs-fridges-should-carry-security-rating-police-chief-says> <<

[57] STUPP, Catherine. «Commission plans cybersecurity rules for internet-connected machines». Euractiv (5 de octubre de 2016). <http://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines>. Dunn, John E. «The EU's latest idea to secure the Internet of Things? Sticky labels». Naked Security (11 de octubre de 2016). <https://nakedse curity. sophos.com/2016/10/11/the-eus-latest-idea-to-secure-the-inter net-of-things-sticky-labels> <<

[58] SADLER, Denham. Security ratings for IoT devices? InnovationAus.com (23 de octubre de 2017). <http://www.innovationaus.com/2017/10/Security-ratings-for-IoT-devices> <<

[59] US Congress. S.1691 Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (1 de agosto de 2017). <https://www.congress.gov/bill/115th-congress/senate-bill/1691/actions>. Chalfant, Morgan. «Dems push for program to secure internet-connected devices». Hill (27 de octubre de 2017). <http://thehill.com/policy/cybersecurity/357509-dems-push-for-program-to-secure-internet-connected-devices> <<

[60] Consumer Reports. Consumer Reports launches digital standard to safeguard consumers' security and privacy in complex marketplace (6 de marzo de 2017). <https://www.consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_ <<

[61] CARDOZO, Nate et al. Who Has Your Back? 2017. Electronic Frontier Foundation (Julio de 2017). <https://www.eff.org/files/2017/07/08/whohasyourback_2017.pdf> <<

[62] MACKINNON, Rebecca et al. 2017 corporate accountability in dex. Ranking Digital Rights (Marzo de 2017). <https://rankingdigitalrights.org/index2017/assets/static/download/RDRindex2 <<

[63] Peiter Mudge Zatko tiene muy buenas ideas sobre este tema y ha creado un ciberlaboratorio donde testar productos de seguridad. ZETTER, Kim. «A famed hacker is grading thousands of programs and may revo lutionize software in the process». Intercept (29 de julio de 2016). <https://theintercept.com/2016/07/29/a-famed-hacker-is-grading-thousands-of-programs-and-may-revolutionize-software-in-the-process> <<

[64] Foley & Lardner LLP. State data breach notification laws (17 de enero de 2018). <https://www.foley.com/state-data-breach-notification-laws> <<

[65] LARSON, Selena. «Senators introduce data breach disclosure bill». CNN (1 de diciembre de 2017). <http://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html> <<

[66] Los resultados han sido heterogéneos. Por ejemplo, sabemos que, si bien una filtración de datos tiene efectos a corto plazo en una empresa, el impacto sobre el precio de las acciones tras dos semanas es mínimo. LANGE, Russell; Burger, Eric W. «Long-term market implications of data breaches, not». Journal of Information Privacy and Security (27 de diciembre de 2017). <http://www.tandfonline.com/doi/full/10.1080/15536548.2017.1394070> <<

[67] US Department of Homeland Security. Stop.Think.Connect <https://www.dhs.gov/stopthinkconnect> [Consulta 24 abril 2018] <<

[68] SCHNEIER, Bruce. «Security design: Stop trying to fix the user». IEEE Security & Privacy (Septiembre-octubre de 2013). <https://www.schneier.com/blog/archives/2016/10/security_design.html> <<

[69] Aquí hay algunos ejemplos: IEEE.computer Society Certification and Credential Program. <https://www.computer.org/web/education/certifications> [Consulta 24 abril 2018]. Association for Computing Machinery. Skillsoft Learning Collections. <https://learning.acm.org/e-learning/skillsoft> [Consulta 24 abril 2018]. (ISC)2. (ISC)2 information security certifications . <https://www.isc2.org/Certifications> [Consulta 24 abril 2018] <<

[70] International Organization for Standardization. ISO/IEC 27000 family: Information security management systems. <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> [Consulta 24 abril 2018] <<

[71] PEELER, Julie; Messer, Angela. «(ISC)2 study: Workforce shortfall due to hiring difficulties despite rising salaries, increased budgets and high job satisfaction rate». (ISC)2 Blog (17 de abril de 2015). <http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-diffi culties-despite-rising-salaries-increased-budgets-a.html>. Kauflin, Jeff. «The fast-growing job with a huge skills gap: Cyber security». Forbes (16 de marzo de 2017). <https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security>. ISACA. 2016 cybersecurity skills gap (Enero de 2016). <https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg>. MORGAN, Steve. Cybersecurity jobs report: 2017 edition. Herjavec Group (2017). <https://www.herjavecgroup.com/wp-content/uploads/2017/06/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf> <<

[72] OLTSIK, John. «Research confirms the cybersecurity skills shortage is an existential threat». CSO (14 de noviembre de 2017). <https://www.csoonline.com/article/3237049/security/research-confirms-the-cybersecurity-skills-shortage-is-an-existential-threat.html> <<

[73] GOODMAN, Mark. «We need a Manhattan project for cyber security». Wired (21 de enero de 2015). <https://www.wired.com/2015/01/we-need-a-manhattan-project-for-cyber-security> <<

[74] Accenture. Defining a cyber moon shot (2 de octubre de 2017). <https://www.accenture.com/t20171004T064630Z__w__/us-en/_acnmedia/PDF-62/Accenture-Defining-Cyber-Moonshot-POV.pdf> <<

[1] BOWERS, Faye. «Building a 747: 43 days and 3 million fasteners». *Christian Science Monitor* (29 de octubre de 1997). <https://www.csmonitor.com/1997/1029/102997.us.us.2.html> <<

[2] Mi velocidad promedio es de 27 millas (43 kilómetros) por hora. Eso en un año tranquilo para mí; en 2015, mi media fue de 33 millas (53 kilómetros) por hora <<

[3] Este es un buen resumen: Hansen, Mark; McAndrews, Carolyn; Berkeley, Emily. History of aviation safety oversight in the United States. DOT/FAA/AR-08-39, National Technical Information Service (Julio de 2008). <http://www.tc.faa.gov/its/worldpac/techrpt/ar0839. pdf> <<

[4] El trayecto en taxi hasta el aeropuerto es la parte más peligrosa del viaje <<

[5] Aquí hay un ejemplo: Coalition for Cybersecurity and Policy and Law. New whitepaper: Building a national cybersecurity strategy: Voluntary, flexible frameworks. Center for Responsible Enterprise and Trade (26 de octubre de 2017). <https://create.org/news/new-whitepaper-building-national-cybersecurity-strategy> <<

[6] GLASER, April. «Federal privacy laws won’t necessarily protect you from spying drones». Recode (15 de marzo de 2017). <https://www.recode.net/2017/3/15/14934050/federal-privacy-laws-spying-drones-senate-hearing> <<

[7] HAFNER, Katie. «And if you liked the movie, a Netflix contest may reward you handsomely». New York Times (2 de octubre de 2006). <http://www.nytimes.com/2006/10/02/technology/02netflix.html> <<

[8] NARAYANAN, Arvind; Shmatikov, Vitaly. «Robust de-anonymization of large sparse datasets». 2008 IEEE Symposium on Security and Privacy (SP '08) (18 de mayo de 2008). <https://dl.acm.org/citation.cfm?id=1398064> <<

[9] OHM, Paul. «Broken promises of privacy: Responding to the surprising failure of anonymization». UCLA Law Review 57 (13 de agosto de 2009). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006> <<

[10] SINGEL, Ryan. «Netflix cancels recommendation contest after privacy lawsuit». Wired (12 de marzo de 2010). <https://www.wired.com/2010/03/netflix-cancels-contest> <<

[11] Esta idea está más desarrollada aquí: HATHAWAY, Melissa E.; Stewart, John N. «Taking control of our cyber future». Georgetown Journal of International Affairs (25 de julio de 2014). <https://www.geor getownjournalofinternationalaffairs.org/online-edition/cyber-iv-featu re-taking-control-of-our-cyber-future> <<

[12] LEVERETT, Eireann; Clayton, Richard; ANDERSON, Ross. Standardization and certification of the 'Internet of Things'. Institute for Consumer Policy (6 de junio de 2017). <https://www.conpolicy.de/en/news-detail/standardization-and-certification-of-the-internet-of-things> <<

[13] BRACY, Jedidiah. McSweeny, SOLTANI, and regulating the IoT. International Association of Privacy Professionals (7 de abril de 2016). <https://iapp.org/news/a/mcsweeney-soltani-and-regulating-the-iot> <<

[14] CALO, Ryan. The case for a federal robotics commission. Brookings Institution (15 de septiembre de 2014). <https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission> <<

[15] SCHERER, Matthew U. «Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies». Harvard Journal of Law & Technology 29, núm. 2 (Spring 2016). <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf> <<

[16] National Cyber Bureau. Mission of the bureau. Prime Minister’s Office (2 de junio de 2013). <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthoriti <<

[17] National Cyber Security Centre. About the NCSC (9 de junio de 2017). <https://www.ncsc.gov.uk/information/about-ncsc> [Consulta 24 abril 2018] <<

[18] ODLYZKO, Andrew. «Network neutrality, search neutrality, and the never-ending conflict between effi-ciency and fairness in markets». Review of Network Economics 8, núm. 1 (1 de marzo de 2009). <https://www.degruyter.com/view/j/rne.2009.8.issue-1/rne.2009.8.1.1169/rne.2009.8.1.1169.xml> <<

[19] Food and Drug Administration. The FDA's role in medical device cybersecurity. <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684 [Consulta 24 abril 2018] <<

[20] ORNSTEIN, Charles. «Federal privacy law lags far behind personal-health technologies». Washington Post (17 de noviembre de 2015). <https://www.washingtonpost.com/news/to-your-health/wp/2015/11/17/federal-privacy-law-lags-far-behind-personal-health-technolo gies> <<

[21] BRANDOM, Russell. «Body blow: How 23andMe brought down the FDA's wrath». Verge (25 de noviembre de 2013). <https://www.theverge.com/2013/11/25/5144928/how-23andme-brought-down-fda-wrath-personal-genetics-wojcicki>. Kolata, Gina. «F.D.A. will allow 23andMe to sell genetic tests for disease risk to consumers». New York Times (6 de abril de 2017). <https://www.nytimes.com/2017/04/06/health/fda-genetic-tests-23andme.html> <<

[22] Electronic Privacy Information Center. FTC v. Wyndham (24 de agosto de 2015). <https://epic.org/amicus/ftc/wyndham> <<

[23] Federal Trade Commission. Wyndham settles FTC charges it unfairly placed consumers' payment card information at risk (9 de diciembre de 2015). <https://www.ftc.gov/news-events/press-relea ses/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-con su mers-payment> <<

[24] CONSTINE, Josh. Facebook now has 2 billion monthly users… and responsibility. TechCrunch (27 de junio de 2017). <https://techcrunch.com/2017/06/27/facebook-2-billion-users> <<

[25] HINZ, Eric R. «A distinction-less distinction: Why the RCS/ECS distinction in the Stored Communications Act does not work». Notre Dame Law Review 88, núm. 1 (1 de noviembre de 2012). <https://scholarship.law.nd.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1115&context=ndlr> <<

[26] KRAVETS, David. «Aging ‘privacy’ law leaves cloud email open to cops». Wired (21 de octubre de 2011). <https://www.wired.com/2011/10/ecpa-turns-twenty-five> <<

[27] SOLON, Olivia; SIDDIQUI, Sabrina. «Forget Wall Street: Silicon Valley is the new political power in Washington». Guardian (3 de septiembre de 2017). <https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington> <<

[28] TAPLIN, Jonathan. «Why is Google spend-ing record sums on lobbying Washington?». Guardian (30 de julio de 2017). <https://www.theguardian.com/technology/2017/jul/30/google-silicon-valley-corporate-lobbying-washington-dc-politics> <<

[29] RUOFF, Alex. Fitness trackers, wellness apps won’t be regulated by FDA. Bureau of National Affairs (29 de julio de 2016). <https://www.bna.com/fitness-trackers-wellness-n73014445597>. Food and Drug Administration, Center for Devices and Radiological Health. General wellness: Policy for low risk devices, guidance for industry and Food and Drug Administration staff. Federal Register (29 de julio de 2016). <https://www.federalregister.gov/documents/2016/07/29/2016-17902/general-wellness-policy-for-low-risk-devices-guidance-for-industry-and-food-and-drug-administration> <<

[30] FUNG, Brian. «What to expect now that Internet providers can collect and sell your Web browser history». Washington Post (29 de marzo de 2017). <https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history> <<

[31] BENKLER, Yochai; COHEN, Julie. «Networks 2» (conference session), After the Digital Tornado Conference. Wharton School, University of Pennsylvania (17 de noviembre de 2017). <http://digitaltornado.net>. Supernova Group. After the Tornado 05: Networks 2. YouTube (19 de noviembre de 2017). <https://www.youtube.com/watch?v=pCGZ8tIrrIU> <<

[32] Las cosas fueron a peor, ya que reemplazó las leyes estatales más duras y eliminó la posibilidad de que la gente presentara demandas. KREBS, Brian. «Is it time to can the CAN-SPAM Act?». KREBS on Security (2 de julio de 2017). <https://krebsonsecurity.com/2017/07/is-it-time-to-can-the-can-spam-act> <<

[33] KATZ, Mitchell J. FTC announces crack-down on two massive illegal robocall operations. Federal Trade Commission (13 de enero de 2017). <https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-crackdown-two-massive-illegal-robocall-operations>. Snider, Mike. «FCC hits robocaller with agency's largest-ever fine of $120 million». USA Today (22 de junio de 2017). <https://www.usatoday.com/story/tech/news/2017/06/22/fcc-hits-robocaller-agencys-largest-ever-fine-120-million/103102546> <<

[34] KATZ, Mitchell J. FTC and DOJ case results in historic decision awarding $280 million in civil penalties against Dish Network and strong injunctive relief for Do Not Call violations. Federal Trade Commission (6 de junio de 2017). <https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil> <<

[35] KATZ, Mitchell J. FTC charges DIRECTV with deceptively advertising the cost of its satellite television service. Federal Trade Commission (11 de marzo de 2015). <https://www.ftc.gov/news-events/press-releases/2015/03/ftc-charges-directv-deceptively-advertising-cost-its-satellite> <<

[36] KANG, Cecilia. «Toymaker VTech settles charges of violating child privacy law». New York Times (8 de enero de 2018). <https://www.nytimes.com/2018/01/08/business/vtech-child-privacy.html> <<

[37] HENDERSON, Juliana Gruenwald. VIZIO to pay $2.2 million to FTC, state of New Jersey to settle charges it collected viewing histories on 11 million smart televisions without users' consent. Federal Trade Commission (6 de febrero de 2017). <https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-sett le-charges-it> <<

[38] Hay diferentes opiniones sobre esto en el área de la seguridad informática. Thierer, Adam. «Avoiding a precautionary principle for the Internet». Forbes (11 de marzo de 2012). <https://www.forbes.com/sites/adamthierer/2012/03/11/avoiding-a-precautionary-principle-for-the-internet>. Stirling, Andy. «Why the precautionary principle matters». Guardian (8 de julio de 2013). <https://www.theguardian.com/science/political-science/2013/jul/08/precautionary-principle-science-policy> <<

[39] Kevin Kelly ha escrito mucho sobre cómo ser prudente a la hora de decidir qué tecnologías debería usar la sociedad y cómo implementarlas. Kelly, Kevin. What Technology Wants. Viking, 2010. <https://books.google.com/books?id=_ToftPd4R8UC> <<

[40] Está empezando. El arresto fue realizado por la policía española y contó con la cooperación del FBI, las autoridades de Rumanía, Bielorrusia y Taiwán y varias empresas de ciberseguridad. Singleton, Micah. «Europol arrests suspects in bank heists that stole $1.2 billion using malware». Verge (26 de marzo de 2018). <https://www.theverge.com/2018/3/26/17165300/europol-arrest-suspect-bank-heists-1-2-bi llion-cryptocurrency-malware> <<

[41] RAYMAN, Noah. «The world’s top 5 cybercrime hotspots». Time (7 de agosto de 2014). <http://time.com/3087768/the-worlds-5-cybercrime-hotspots> <<

[42] KIM, Christine. «North Korea hacking increasingly focused on making money more than espionage: South Korea study». Reuters (27 de julio de 2017). <https://www.reuters.com/article/us-northkorea-cyber crime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO> <<

[43] Council of Europe. Details of Treaty No. 185: Convention on Cybercrime. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> [Consulta 24 abril 2018] <<

[44] STERLING, Bruce. «Respecting Chinese and Russian cyber-sovereignty in the formerly global internet». Wired (22 de diciembre de 2015). <https://www.wired.com/beyond-the-beyond/2015/12/respecting-chine se-and-russian-cyber-sovereignty-in-the-formerly-global-internet>. Limbago, Andrea. «The global push for cyber sovereignty is the beginning of cyber fascism». Hill (13 de diciembre de 2016). <http://thehill.com/blogs/congress-blog/technology/310382-the-global-push-for-cy ber-sovereignty-is-the-beginning-of>. Mikheev, Vladimir. «Why do Beijing and Moscow embrace cyber sovereignty?». Russia beyond the Headlines (22 de marzo de 2017). <https://www.rbth.com/opinion/2017/03/22/why-do-beijing-and-moscow-embrace-cyber-sovereignty_725018> <<

[45] NYE, Joseph S. «Normative restraints on cyber conflict». Cyber Security (próximamente) <<

[46] United Nations General Assembly. «Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security». Resolution A/68/98 (24 de junio de 2013). <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98> <<

[47] SOESANTO, Stefan; D’Incau, Fosca. The UNGGE is dead: Time to fall forward. European Council on Foreign Relations (15 de agosto de 2017). <http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_gov <<

[48] RABKIN, Ariel. Cyber-arms cannot be controlled by treaties. American Enterprise Institute (3 de marzo de 2015). <https://www.aei.org/publication/cyber-arms-cannot-be-controlled-by-treaties> <<

[49] HEALEY, Jason. Risk nexus: Beyond data breaches: Global interconnections of cyber risk . Atlantic Council (Abril de 2014). <http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf> <<

[50] THOMLINSON, Matt. «Microsoft announces Brussels Transparency Center at Munich Security Conference». Microsoft on the Issues (31 de enero de 2014). <https://blogs.microsoft.com/on-the-issues/2014/01/31/microsoft-announces-brussels-transparency-center-at-munich-securi ty-conference> <<

[51] SMITH,, Brad. «The need for a Digital Geneva Convention». Microsoft on the Issues (14 de febrero de 2017). <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention> <<

[52] WALKER, Kent. Digital security and due process: Modernizing cross-border government access standards for the cloud era. Google (31 de octubre de 2017). <https://blog.google/documents/2/CrossBorderLawEnforcementRequestsWhit<<

[1] HEALEY, Jason. «A nonstate strategy for saving cyberspace». *Atlantic Council Strategy Paper* núm. 8, Atlantic Council (Enero de 2017). <http://www.atlanticcouncil.org/images/publications/AC_StrategyPapers_No8 <<

[2] FERRIS, John. «Signals intelligence in war and power politics, 1914-2010». The Oxford Handbook of National Security Intelligence. Oxford, 2010. <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195375886.0 9780195375886-e-0010> <<

[3] DANCHEV, Dancho. «Black market for zero day vulnerabilities still thriving». ZDNet (2 de noviembre de 2008). <http://www.zdnet.com/blog/security /black-market-for-zero-day-vulnerabilities-still-thriving/2108>. Patterson, Dan. «Gallery: The top zero day Dark Web markets». TechRepublic (9 de enero de 2017). <https://www.techrepublic.com/pictures/gallery-the-top-zero-day-dark-web-markets> <<

[4] GREENBERG, Andy. «Meet the hackers who sell spies the tools to crack your PC (and get paid six-figure fees)». Forbes (21 de marzo de 2012). <http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees> <<

[5] COX, Joseph; FRANCESCHI-BICCJIERAI, Lorenzo. «How a tiny startup became the most important hacking shop you've never heard of». Vice Motherboard (7 de febrero de 2018). <https://motherboard.vice.com/en_us/article/8xdayg/iphone-zero-days-inside-azimuth-security> <<

[6] SEGAL, Adam. Using incentives to shape the zero-day market. Council on Foreign Relations (19 de septiembre de 2016). <https://www.cfr.org/report/using-incentives-shape-zero-day-market> <<

[7] Tor Project. Policy [re Tor bug bounties]. Hacker One, Inc. (last updated 20 de septiembre de 2017). <https://hackerone.com/torproject> <<

[8] Zerodium. Tor browser zero-day exploits bounty (13 de septiembre de 2017; expired 1 de diciembre de 2017). <https://zerodium.com/tor.html> <<

[9] GOLDSMITH, Jack. «Cyber paradox: Every offensive weapon is a (potential) chink in our defense and viceversa». Lawfare (12 de abril de 2014). <http://www.lawfareblog.com/2014/04/cyber-paradox-every-offensive-weapon-is-a-potential-chink-in-our-defense-and-vice-versa> <<

[10] BRENNER, Joel. «The policy tension on zero-days will not go away». Lawfare (14 de abril de 2014). <http://www.lawfareblog.com/2014/04/the-policy-tension-on-zero-days-will-not-go-away> <<

[11] DOCTOROW, Cory. «If GCHQ wants to improve national security it must fix our technology». Guardian (11 de marzo de 2014). <http://www.theguardian.com/technology/2014/mar/11/gchq-national-security-technology> <<

[12] SCHNEIER, Bruce. «It’s time to break up the NSA». CNN (20 de febrero de 2014). <http://edition.cnn.com/2014/02/20/opinion/schneier-nsa-too-big/index.html> <<

[13] GEER, Dan. Three policies (3 de abril de 2013). <http://geer.tinho.net/three.policies.2013Apr03Wed.PDF> <<

[14] SMITH, Brad. «The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack». Microsoft on the Issues (14 de mayo de 2017). <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack> <<

[15] WEST, Heather. «Mozilla statement on CIA/WikiLeaks». Open Policy & Advocacy (7 de marzo de 2017). < https://blog.mozilla.org/netpolicy/2017/03/07/mozilla-statement-on-cia-wikileaks>. Ben-Avie, Jochai. «Vulnerability disclosure should be part of new EU cybersecurity strategy». Open Policy & Advocacy (3 de octubre de 2017). <https://blog.mozilla.org/netpolicy/2017/10/03/vulnerability-disclosure-should-be-in-new-eu-cybersecurity-strategy> <<

[16] CLARKE,, Richard A. et al. Liberty and security in a changing world . President's Review Group on Intelligence and Communications Technologies (12 de diciembre de 2013). <https://obamawhite house.archives.gov/sites/default/files/docs/2013-12-12_rg_final_re port.pdf> <<

[17] TANto la NSA como el FBI han dado las mismas razones. SANGER, David E. «White House details thinking on cybersecurity flaws». New York Times (28 de abril de 2014). <http://www.nytimes.com/2014/04/29/us/white-house-details-thinking-on-cybersecuri ty-gaps.html> <<

[18] LEDGETT, Rick. «No, the U.S. government should not disclose all vulnerabilities in its possession». Lawfare (7 de agosto de 2017). <https://www.lawfareblog.com/no-us-government-should-not-disclose-all-vulnerabilities-its-possession> <<

[19] PETERSON, Andrea. «Why everyone is left less secure when the NSA doesn't help fix security flaws». Washington Post (4 de octubre de 2013). <https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws> <<

[20] NEWMAN, Lily Hay. «Why governments won’t let go of secret software bugs». Wired (16 de junio de 2017). <https://www.wired.com/2017/05/governments-wont-let-go-secret-software-bugs> <<

[21] DANIEL, Michael. Heartbleed: Understanding when we disclose cyber vulnerabilities. Office of the President of the United States (28 de abril de 2014). <http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities> <<

[22] CROCKER, Andrew. EFF pries more information on zero days from the government's grasp. Electronic Frontier Foundation (19 de enero de 2016). <https://www.eff.org/deeplinks/2016/01/eff-pries-more-transparency-zero-days-governments-grasp> <<

[23] Office of the President of the United States. Vulnerabilities equities policy and process for the United States government (15 de no viembre de 2017). <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>. JOYCE, Rob. «Improving and making the vulnerability equities process transparent is the right thing to do». Wayback Machine (15 de noviembre de 2017). <https://web.archive.org/web/20171115151504/https://www.whitehouse.gov/b and-making-vulnerability-equities-process-transparent-right-thing-do> <<

[24] NAKASHIMA, Ellen; TIMBERG, Craig. «NSA officials worried about the day its potent hacking tool would get loose. Then it did». Washington Post (16 de mayo de 2017). <https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html> <<

[25] La NSA al final dio a conocer la vulnerabilidad, pero después de que los rusos la robaran. GOODIN, Dan. «Fearing Shadow Brokers leak, NSA reported critical flaw to Microsoft». Ars Technica (17 de mayo de 2017). <https://arstechnica.com/information-technology/2017/05/fearing-shadow-brokers-leak-nsa-reported-critical-flaw-to-microsoft> <<

[26] GREENBERG, Andy. «Triple Meltdown: How so many researchers found a 20-year-old chip flaw at the same time». Wired (7 de enero de 2018). <https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery> <<

[27] En 2017, traté de estimar la tasa anual de redescubrimiento utilizando los datos disponibles y encontré que estaba entre el 11 % y el 22 %. Por otro lado, un grupo de investigadores de la Corporación RAND trató de estimarla también utilizando distintos supuestos y otros datos; encontraron que la tasa era inferior al 6 %. Somos ciegos tocando diferentes partes de un elefante. Cada uno extrapola a partir de sus propios datos. Queda claro que no vamos a saber mucho sobre las capacidades de la NSA de esta manera. Herr, Trey; SCHNEIER, Bruce; MORRIS, Christopher. «Taking stock: Estimating vulnerability recovery». Belfer Cyber Security Project White Paper Series. Harvard Kennedy School Belfer Center for Science and International Affairs (7 de marzo de 2017). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928758>. Ablon, Lillian; Bogart, Timothy. Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits. RAND Corporation (9 de marzo de 2017). <https://www.rand.org/pubs/research_reports/RR1751.html> <<

[28] SHANE, Scott; ROSENBERG, Matthew; LEHREN, Andrew W. «WikiLeaks releases trove of alleged C.I.A. hacking documents». New York Times (7 de marzo de 2017). <https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html>. <https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html>. SHANE, SCOTT; PERLROTH,, Nicole; SANGER, David E. «Security breach and spilled secrets have shaken the N.S.A. to its core». New York Times (12 de noviembre de 2017). <https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html> <<

[29] SCHNEIER, Bruce. «Zero-day vulnerabilities against Windows in the NSA tools released by the Shadow Brokers». Schneier on Security (28 de julio de 2017). <https://www.schneier.com/blog/archives/2017/07/zero-day_vulner.html> <<

[30] GOODIN, Dan. «Mysterious Microsoft patch killed 0-days released by NSA-leaking Shadow Brokers». Ars Technica (16 de abril de 2017). <https://arstechnica.co.uk/information-technology/2017/04/purported-shadow-brokers-0days-were-in-fact-killed-by-mysterious-patch> <<

[31] National Security Agency/Central Security Service. Discovering IT problems, developing solutions, sharing expertise (30 de octubre de 2015). <https://www.nsa.gov/news-features/news-stories/2015/discovering-solving-sharing-it-solutions.shtml> <<

[32] HEALEY, Jason. «The U.S. government and zero-day vulnerabilities: From pre-Heartbleed to the Shadow Brokers». Columbia Journal of International Affairs (1 de noviembre de 2016). <https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process> <<

[33] SCHNEIER, Bruce. «Should U.S. hackers fix cybersecurity holes or exploit them?». Atlantic (19 de mayo de 2014). <https://www.schneier.com/essays/archives/2014/05/should_us_hackers_fi.htr SCHWARTZ, Ari; Knake, Rob. Government's role in vulnerability disclosure: Creating a permanent and accountable vulnerability equities pro cess. Harvard Kennedy School Belfer Center for Science and Internatio nal Affairs (1 de junio de 2016). <https://www.belfercenter.org/publication/governments-role-vulnerability-disclosure-creating-per manent-and-accountable>. HEALEY, Jason. «The U.S. government and zero-day vulnerabilities: From pre-Heartbleed to the Shadow Brokers». Columbia Journal of International Affairs (1 de noviembre de 2016). <https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_ equities_process> <<

[34] FALKOWITZ,, Oren J. «U.S. cyber policy makes Americans vulnerable to our own government». Time (10 de enero de 2017). <http://time.com/4625798/donald-trump-cyber-policy> <<

[35] GILMORE,, John. «Re: [Cryptography] opening discussion: Speculation on ‘BULLRUN’». Mail Archive (6 de septiembre de 2013). <https://www.mail-archive.com/cryptography@@metzdowd.com/msg12325. html> <<

[36] FERGUSON, Niels; SCHNEIER, Bruce. «A cryptographic evaluation of Ipsec». Counterpane Internet Security (Diciembre de 2003). <https://www.schneier.com/academic/paperfiles/paper-ipsec.pdf> <<

[37] BARKAN, Elad; Biham, Eli; Keller, Nathan. Instant ciphertext-only cryptanalysis of GSM encrypted communication (17 de septiembre de 2003). <http://cryptome.org/gsm-crack-bbk.pdf> <<

[38] PERLROTH, Nicole; LARSON, Jeff; SHANE, SCOTT. «Secret docu ments reveal N.S.A. campaign against encryption». New York Times (5 de septiembre de 2013). <http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryp tion.html>. PERLROTH, Nicole; LARSON, Jeff; SHANE, Scott. «N.S.A. able to foil basic safeguards of privacy on web». New York Times (5 de septiem bre de 2013). <http://www.nytimes.com/2013/09/06/us/nsa-foi ls-much-internet-encryption.html>. Ball, Julian; Borger, Julian; GREENWALD, Glenn. «Revealed: How US and UK spy agencies defeat internet privacy and security». Guardian (6 de septiembre de 2013). <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> <<

[39] GIDARI, Albert. More CALEA and why it trumps the FBI's All Writs Act order. Center for Internet and Society, Stanford Law School (22 de febrero de 2016). <http://cyberlaw.stanford.edu/blog/2016/02/more-calea-and-why-it-trumps-fbis-all-writs-act-order> <<

[40] InfoSec Institute. Cellphone surveillance: The secret arsenal (8 de enero de 2016). <http://resources.infosecinstitute.com/cellphone-surveillance-the-secret-arsenal> <<

[41] HRUSKA, Joel. «Stingray, the fake cell phone tower cops and carriers use to track your every move». Extreme Tech (17 de junio de 2014). <http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move> <<

[42] ZETTER, Kim. «Emails show feds asking Florida cops to deceive judges». Wired (19 de junio de 2014). <http://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray> <<

[43] WESSLER, Nathan Freed. U.S. marshals seize local cops' cell phone tracking files in extraordinary attempt to keep information from public. American Civil Liberties Union (3 de junio de 2014). <https://www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-sei ze-local-cops-cell-phone-tracking-files> <<

[44] PATRICK, Robert. «Controversial secret phone tracker figured in dropped St. Louis case». St. Louis Post-Dispatch (19 de abril de 2015). <http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_ fbb82630-aa7f-5200-b221-a7f90252b2d0.html>. FARIVAR, Cyrus. «Robbery suspect pulls guilty plea after stingray disclosure, case dropped». Ars Technica (29 de abril de 2015). <http://arstechnica.com/tech-poli cy/2015/04/29/alleged-getaway-driver-challenges-stingray-use-rob bery-case-dropped> <<

[45] PELL, Stephanie K.; Soghoian, Christopher. «Your secret Stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy». Harvard Journal of Law and Technology 28, núm. 1 (29 de diciem bre de 2014). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678> <<

[46] ZETTER, Kim. «Hacker spoofs cell phone tower to intercept calls». Wired (21 de julio de 2010). <http://www.wired.com/2010/07/intercepting-cell-phone-calls> <<

[47] SOLTANI, Ashkan; TIMBERG, Craig. «Tech firm tries to pull back curtain on surveillance efforts in Washington». Washington Post (17 de septiembre de 2014). <http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html> <<

[48] Un tal Sr. Mark Lazarte vende un receptor PKI1640IMSI por 1.800 dólares. Parece estar hecho en Guangdong (China). Lazarte, Mark. «IMSI catcher». Alibaba. <https://www.alibaba.com/product-detail/IMSI-catcher_135958750.html> [Consulta 24 de abril de 2018] <<

[49] SAVAGE, Charlie et al. «Hunting for hackers, NSA secretly expands Internet spying at U.S. border». New York Times (4 de junio de 2015). <https://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html> <<

[50] PREVALAKIS, Vassilis; SPINELLIS, Diomidis. «The Athens affair». IEEE Spectrum (29 de junio de 2007). <https://spectrum.ieee.org/telecom/security/the-athens-affair> <<

[51] CROSS, Tom. «Exploiting lawful intercept to wiretap the Internet». Black Hat DC 2010 (3 de febrero de 2010). <http://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-wp.pdf> <<

[52] Citado en LANDAU, Susan (1 de marzo de 2016). Testimony for House Judiciary Committee hearing on 'The encryption tightrope: Rebalancing Americans' security and privacy'. <https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf> <<

[53] PETERSON, Andrea. «Why everyone is left less secure when the NSA doesn’t help fix security flaws». Washington Post (4 de octubre de 2013). <https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws> <<

[54] HAYDEN, Michael V. The equities decision: Deciding when to exploit or defend. Chertoff Group (17 de mayo de 2017). <http://www.chertoffgroup.com/point-of-view/109-the-chertoff-group-point-of-view/665-the-equities-decision-deciding-when-to-exploit-or-defend> <<

[55] ABELSON, Harold et al. «Keys under doormats: Mandating insecurity by requiring government access to all data and communications». MIT CSAIL Technical Report 2015-026, MIT Computer Science and Artificial Intelligence Laboratory (7 de julio de 2015). <https://dspace.mit.edu/handle/1721.1/97690> <<

[56] He oído que se conoce como la sucursal de GCHQ en Londres <<

[57] NAKASHIMA, Ellen. «National Security Agency plans major reorganization». Washington Post (2 de febrero de 2016). <https://www.washingtonpost.com/world/national-security/national-security-agen cy-plans-major-reorganization/2016/02/02/2a66555e-c960-11e5-a7b2-5a2f824b02c9_story.html> <<

[58] Nicholas Weaver trata muy bien este punto. Weaver, Nicholas. «Trust and the NSA reorganization». Lawfare (10 de febrero de 2016). <https://www.lawfareblog.com/trust-and-nsa-reorganization> <<

[59] MASUNAGA, Samantha. «FBI doesn't have to say who unlocked San Bernardino shooter's iPhone, judge rules». Los Angeles Times (2 de octubre de 2017). <http://beta.latimes.com/business/la-fi-tn-fbi-iphone-20171002-story.html> <<

[60] KHAMOOSHI, Arash. «Breaking down Apple's iPhone fight with the U.S. government». New York Times (3 de marzo de 2016). <https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html> <<

[61] FOX-BREWSTER, Thomas. «The feds can now (probably) unlock every iPhone model in existence». Forbes (26 de febrero de 2018). <https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite>. GALLAGHER, Sean. «Cellebrite can unlock any iPhone (for some values of 'any')». Ars Technica (28 de febrero de 2018). <https://arstechnica.com/information-technology/2018/02/cellebrite-can-unlock-any-iphone-for-some-values-of-any> <<

[62] ZAPOTOSKY, Matt. «FBI has accessed San Bernardino shooter's phone without Apple help». Washington Post (28 de marzo de 2016). <https://www.washingtonpost.com/world/national-security/fbi-has-ac cessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html>. KRAVETS, David. «FBI may keep secret the name of vendor that cracked terrorist's iPhone». Ars Technica (1 de octubre de 2017). <https://arstechnica.com/tech-policy/2017/10/fbi-does-not-have-to-disclose-payments-to-vendor-for-iphone-cracking-tool> <<

[63] ZITTRAIN, Jonathan et al. Don’t panic: Making progress on the ‘going dark’ debate. Berkman Center for Internet and Society, Harvard University (Febrero de 2016). <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate. pdf> <<

[64] LANDAU, Susan. Listening In: Cybersecurity in an Insecure Age. Yale University Press, 2017. <https://books.google.com/books?id=QZ47DwAAQBAJ> <<

[65] LANDAU, Susan. Testimony for House Judiciary Committee hearing on ‘The encryption tightrope: Rebalancing Americans’ security and privacy’ (1 de marzo de 2016). <https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf> <<

[66] BELLOVIN, Steven M. et al. «Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet». Northwestern Journal of Technology and Intellectual Property 12, núm. 1 (19 de agosto de 2014). <https://www.ssrn.com/abstract=2312107> <<

[67] Lo están intentando. Federal Bureau of Investigation. Most wanted talent: Seeking tech experts to become cyber special agents (29 de diciembre de 2014). <https://www.fbi.gov/news/stories/fbi-seeking-tech-experts-to-become-cyber-special-agents> <<

[68] ROBINSON, Neil; Disley, Emma. Incentives and challenges for information sharing in the context of network and information security. European Network and Information Security Agency (10 de septiembre de 2010). <https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing/at_download/fullReport> <<

[69] GORDON, LAWRENCE A.; LOEB, MARTIN P.; Lucyshyn, William. «Sharing information on computer systems security: An economic analysis». Journal of Accounting and Public Policy 22, núm. 6 (Febrero de 2003). <http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.598.6498&rep=rep1&type=pdf> <<

[70] US Department of Homeland Security. Enhancing resilience through cyber incident data sharing and analysis (10 de septiembre de 2015). <https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20%20508%20compliant.pdf> <<

[71] BAIR, Jonathan et al. «That was close! Reward reporting of cybersecurity 'near misses'» (próximamente). Colorado Technology Law Journal 16, núm. 2. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081216> <<

[72] ROBINSON, Neil. «The case for a cyber-security safety board: A global view on risk». RAND Blog (19 de junio de 2012). <https://www.rand.org/blog/2012/06/the-case-for-a-cyber-security-safety-board-a-global.html> <<

[73] National Transportation Safety Board. 2017-2018 most wanted list. <https://www.ntsb.gov/safety/mwl/Pages/default.aspx> [Consulta 24 abril 2018] <<

[74] ROTHKE, Ben. «It’s time for a National Cybersecurity Safety Board (NCSB)». CSO (19 de febrero de 2015). <https://www.csoonline.com/article/2886326/security-awareness/it-s-time-for-a-national-cybersecurity-safety-board-ncsb.html> <<

[75] KERNER, Sean Michael. «Cyber Threat Alliance adds new members to security sharing group». eWeek (27 de octubre de 2017). <http://www.eweek.com/security/cyber-threat-alliance-adds-new-members-to-security-sharing-group> <<

[76] Estados Unidos acusó a cinco miembros del Ejército Popular de Liberación chino por estos ataques en 2014. Schmidt, Michael S.; SANGER, David E. «5 in China army face U.S. charges of cyberattacks». New York Times (19 de mayo de 2014). <https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html> <<

[77] GAOUETTE, Nicole. «FBI's COMEY: Republicans also hacked by Russia». CNN (10 de enero de 2017). <http://www.cnn.com/2017/01/10/politics/comey-republicans-hacked-russia/index.html> <<

[78] En 2017, el diputado Will Hurd propuso esto. Konkel, Frank. «Lawmaker: Cyber National Guard could fill federal workforce gaps». Nextgov (21 de junio de 2017). <http://www.nextgov.com/cybersecurity/2017/06/lawmaker-cyber-national-guard-could-fill-federal-workforce-gaps/138851> <<

[79] RUIZ, Monica M. «Is Estonia's approach to cyber defense feasible in the United States?». War on the Rocks (9 de enero de 2018). <https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states> <<

[1] MATISHAK, Martin. «After Equifax breach, anger but no action in Congress». *Politico* (1 de enero de 2018). <https://www.politico.com/story/2018/01/01/equifax-data-breach-congress-action-319631> <<

[2] CcLean, Robert. «Elizabeth Warren's Equifax bill would make credit freezes free». CNN (15 de septiembre de 2017). <http://money.cnn.com/2017/09/15/pf/warren-schatz-equifax/index.html> <<

[3] COLDEWEY, Devin. «Congress votes to disallow consumers from suing Equifax and other companies with arbitration agreements». TechCrunch (24 de octubre de 2017). <https://techcrunch.com/2017/10/24/congress-votes-to-disallow-consumers-from-suing-equifax-and-other-companies-with-arbitration-agreements/amp> <<

[4] WARNER, Mark R. Senators introduce bipartisan legislation to improve cybersecurity of ‘Internet of things’ (IoT) devices (1 de agosto de 2017). <https://www.warner.senate.gov/public/index.cfm/2017/8/ena tors-introduce-bipartisan-legislation-to-improve-cybersecurity-of-in ternet-of-things-iot-devices> <<

[5] OBAMA, Barack. Presidential executive order: Commission on Enhancing National Cybersecurity. Office of the President of the United States (9 de febrero de 2016). <https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity> <<

[6] DONILON, Thomas E. et al. *Report on securing and growing the digital economy*. Commission on Enhancing National Cybersecurity (1 de diciembre de 2016). <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf> <<

[7] TRUMP, Donald J. Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure. Office of the President of the United States (11 de mayo de 2017). <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure> <<

[8] MARINOS, Nick. Critical infrastructure protection: Additional actions are essential for assessing cybersecurity framework adoption, GAO-18-211. US Government Accountability Office (13 de febrero de 2018). <https://www.gao.gov/assets/700/690112.pdf> <<

[9] Puedes culpar a una Administración disfuncional, pero no creo que hubiera ido mucho mejor en cualquier otra <<

[10] Economist. «How to manage the computer-security threat». Economist (8 de abril de 2017). <https://www.economist.com/news/lea ders/21720279-incentives-software-firms-take-security-se riously-are-too-weak-how-manage> <<

[11] JENSEN, Christopher. «50 years ago, Unsafe at Any Speed shook the auto world». New York Times (26 de noviembre de 2015). <https://www.nytimes.com/2015/11/27/automobiles/50-years-ago-unsafe-at-any-speed-shook-the-auto-world.html> <<

[12] European Union. «Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)». Official Journal of the European Union (27 de abril de 2016). <http://eur-lex.europa.eu/eli/reg/2016/679/oj> <<

[13] Este es un buen resumen: Bowles, Cennydd. A techie’s rough guide to GDPR (12 de enero de 2018). <https://www.cennydd.com/writing/a-techies-rough-guide-to-gdpr> <<

[14] SCOTT, Mark; Cerulus, Laurens. «Europe's new data protection rules export privacy standards worldwide». Politico (31 de enero de 2018). <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation> <<

[15] Esto ya está sucediendo como respuesta a la GDPR, PayPal publicó una lista de seiscientas empresas con las que compartía los datos de sus usuarios. Desactivaron la página, pero la información se ha guardado. Ricks, Rebecca. How PayPal shares your data. <https://rebecca-ricks.com/paypal-data> [Consulta 24 abril 2018] <<

[16] SCOTT, Mark; Cerulus, Laurens. «Europe's new data protection rules export privacy standards worldwide». Politico (31 de enero de 2018). <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation> <<

[17] BOULTON, Clint. «U.S. companies spending millions to satisfy Europe's GDPR». CIO (26 de enero de 2017). <https://www.cio.com/article/3161920/privacy/article.html>. Ismail, Nick. «Only 43 % of organisations are preparing for GDPR». Information Age (2 de mayo de 2017). <http://www.information-age.com/43-organisations-preparing-gdpr-123465995>. GORDON, Sarah. «Businesses failing to prepare for EU rules on data protection». Financial Times (18 de junio de 2017). <https://www.ft.com/content/28f4eff8-51bf-11e7-a1f2-db19572361bb> <<

[18] EUGDPR.org. GDPRkeychanges. <https://www.eugdpr.org/key-changes.html> [Consulta 24 abril 2018] <<

[19] SCOTT, Mark. «Google fined record $2.7 billion in E.U. antitrust ruling». New York Times (27 de junio de 2017). <https://www.nytimes.com/2017/06/27/technology/eu-google-fine.html>. WHITE, Aoife; Bergen, Mark. «Google to comply with EU search demands to avoid more fines». Bloomberg (29 de agosto de 2017). <https://www.bloomberg.com/news/articles/2017-08-29/google-faces-tuesday-deadline-as-clock-ticks-toward-new-eu-fines> <<

[20] TSUKAYAMA, Hayley. «Facebookwill pay $122 million in fines to the E.U.». Washington Post (18 de mayo de 2017). <https://www.washingtonpost.com/news/the-switch/wp/2017/05/18/facebook-will-pay-122-million-in-fines-to-the-eu> <<

[21] ROBERTS, Paul. «Hilton was fined $700K for a data breach. Under GDPR it would be $420M». Digital Guardian (2 de noviembre de 2017). <https://digitalguardian.com/blog/hilton-was-fined-700k-data-breach-under-gdpr-it-would-be-420m> <<

[22] LEVERETT, Eireann; Clayton, Richard; ANDERSON, Ross. Standardization and certification of the 'Internet of Things'. Institute for Con sumer Policy (6 de junio de 2017). <https://www.conpolicy.de/en/news-detail/standardization-and-certification-of-the-internet-of-things> <<

[23] En este sentido, el software es similar a los libros de texto en el mercado estadounidense, donde unos pocos estados controlan lo que está disponible a nivel estatal debido a sus grandes exigencias <<

[24] FARIVAR, Cyrus. «CEO says Facebook will impose new privacy rules ‘everywhere’». Ars Technica (4 de abril de 2018). <https://arstechnica.com/tech-policy/2018/04/ceo-says-facebook-will-impose-new-eu-privacy-rules-everywhere> <<

[25] Kennedy’s Law LLP. Personal data privacy principles in Asia Pacific (20 de abril de 2016). <http://www.kennedyslaw.com/dataprivacyapacguide2016> <<

[26] STAFF, Wire. «Right to privacy a fundamental right, says Supreme Court in unanimous verdict». Wire (24 de agosto de 2017). <https://thewire.in/170303/supreme-court-aadhaar-right-to-privacy> <<

[27] TAN, Bryan. «Singapore finalises new Cybersecurity Act». Out-Law (9 de febrero de 2018). <https://www.out-law.com/en/articles/2018/february/singapore-finalises-new-cybersecurity-act> <<

[28] TENE, Omer. «Israel enacts land-mark data security notification regulations». Privacy Tracker (22 de marzo de 2017). <https://iapp.org/news/a/israel-enacts-landmark-data-security-notification-regulations> <<

[29] EDER, Steve. «Donald TRUMP's hotel chain to pay penalty over data breaches». New York Times (24 de septiembre de 2016). <https://www.nytimes.com/2016/09/25/us/politics/trump-hotel-data.html> <<

[30] GUZMAN-LOPEZ, Adolfo. «California attorney general warns tech companies about mining student data for profit». Southern California Public Radio (2 de noviembre de 2016). <https://www.scpr.org/news/2016/11/02/65908/attorney-general-warns-tech-companies-to-follow-ne> <<

[31] MCKENNA, Francine. «Equifax faces its biggest litigation threat from state attorneys general». MarketWatch (15 de septiembre de 2017). < https://www.marketwatch.com/story/equifax-faces-its-biggest-litigation-threat-from-state-attorneys-general-2017-09-15/print> <<

[32] TIKU, Nitasha. «State attorneys general are Google's next headache». Wired (14 de noviembre de 2017). <https://www.wired.com/story/state-attorneys-general-are-googles-next-headache> <<

[33] ARMENTAL, Maria. «Lenovo reaches $3.5 million settlement over preinstalled adware». MarketWatch (6 de septiembre de 2017). <https://www.marketwatch.com/story/lenovo-reaches-35-million-settle ment-with-ftc-over-preinstalled-adware-2017-09-05> <<

[34] KREBS, Brian. «San Diego sues Experian over ID theft service». KREBS on Security (18 de marzo de 2018). <https://krebsonsecurity.com/2018/03/san-diego-sues-experian-over-id-theft-service> <<

[35] KRIMMINGER, Michael. New York cybersecurity regulations for financial institutions enter into effect. Harvard Law School Forum on Corporate Governance and Financial Regulation (25 de marzo de 2017). <https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institutions-enter-into-effect> <<

[36] BELGUM, Karl D. «Internet of Things legislation in California is dead for this year, but it will be back». Nixon Peabody (21 de junio de 2017). <http://web20.nixonpeabody.com/dataprivacy/Lists/Posts/Post.aspx?ID=1155> <<

[37] EIDAM, Eyragon; MULHOLLAND, Jessica. «10 states take Internet privacy matters into their own hands». Government Technology (10 de abril de 2017). <http://www.govtech.com/policy/10-States-Take-Internet-Privacy-Matters-Into-Their-Own-Hands.html> <<

[38] California Legislative Information. SB-327 Information privacy: Connected devices. <https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180SB327> [Consulta 24 abril 2018] <<

[39] FRIEL, Alan L.; Goldstein, Linda A.; Al Melton, Holly. «AD-ttorneys@@law-January 31, 2018». Baker Hostetler (31 de enero de 2018). <https://www.bakerlaw.com/alerts/ad-ttorneys law-january-31-2018> <<

[40] ZIMA, Elizabeth. «California wants to govern bots and police user privacy on social media». Government Technology (23 de febrero de 2018). <http://www.govtech.com/social/California-Wants-to-Govern-bots-and-Police-User-Privacy-on-Social-Media.html> <<

[41] GAGE, Deborah. «Eight questions to ask before buying an internet-connected device». Wall Street Journal (15 de septiembre de 2017). <https://www.wsj.com/articles/eight-questions-to-ask-before-buying-an-internet-connected-device-1505487931> <<

[42] Aquí hay dos buenos para empezar: Electronic Frontier Foundation Surveillance self-defense (21 de octubre de 2014, last updated 21 de septiembre de 2015). <https://ssd.eff.org>. Motherboard STAFF. «The Motherboard guide to not getting hacked». Vice Motherboard (15 de noviembre de 2017). <https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide> <<

[43] FALKVINGE, Rick. «Worst known governmental leak ever is slowly coming to light: Agency moved nation's secret data to 'the cloud'». Privacy News Online (21 de julio de 2017). <https://www.privateInternetaccess.com/blog/2017/07/swedish-transport-agency-worst-known-governmental-leak-ever-is-slowly-coming-to-light> <<

[44] Por seguridad, usa Signal. Si desconfías de tener Signal en tu teléfono, usa WhatsApp. LEE, Micah. «Battle of the secure messaging apps: How Signal beats WhatsApp». Intercept (22 de junio de 2016). <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp> <<

[45] UCHILL, Joe. «DOJ applies to take Microsoft data warrant case to Supreme Court». Hill (23 de junio de 2017). <http://thehill.com/policy/cybersecurity/339281-doj-applies-to-take-microsoft-data-warrant-case-to-supreme-court> <<

[46] SCHNEIER, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton, 2015. <https://books.google.com/books/?id=MwF-BAAAQBAJ> <<

[1] URBINA, Ian. «Court rejects law limiting online pornography». *New York Times* (23 de marzo de 2007). <www.nytimes.com/2007/03/23/us/23porn.html> <<

[2] Electronic Frontier Foundation. Unintended consequences: Fifteen years under the DMCA (1 de marzo de 2013). <https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca> <<

[3] FREEH, Louis J. The impact of encryption on public safety: Statement of the Director. Federal Bureau of Investigation, before the Permanent Select Committee on Intelligence, United States House of Representatives (9 de septiembre de 1997). <https://fas.org/irp/congress/1997_hr/h970909f.htm> <<

[4] CAPRONI, Valerie. Statement before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security. Federal Bureau of Investigation (17 de febrero de 2011). <https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies> <<

[5] COMEY, James B. Going dark: Encryption, technology, and the balances between public safety and privacy. Federal Bureau of Investiga tion (8 de julio de 2015). <https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy> <<

[6] ROSENSTEIN, Rod J. Deputy Attorney General Rod J. ROSENSTEIN delivers remarks at the Cambridge Cyber Summit. US Department of Justice (4 de octubre de 2017). <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cy ber-summit> <<

[7] Peter Swire y Kenesa Ahmad son los responsables de este término. Swire, Peter; Ahmad, Kenesa. ‘ Going dark’ versus a ‘golden age for surveillance ’. Center for Democracy and Technology (28 de noviembre de 2011). <https://cdt.org/blog/%E2%80%98going-dar k%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillan ce%E2%80%99> <<

[8] WILSON, Andi; KEHL, Danielle; Bankston, Kevin. Doomed to repeat history? Lessons from the crypto wars of the 1990s. New America Foundation (17 de junio de 2015). <https://www.newamerica.org/oti/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s> <<

[9] Federal Bureau of Investigation. Encryption: Impact on law enforcement (3 de junio de 1999). <https://web.archive.org/web/20000815210233/https://www.fbi.gov/library/en <<

[10] NAKASHIMA, Ellen. «FBI director: Tech companies should be required to make devices wiretap-friendly». Washington Post (16 de octubre de 2014). <https://www.washingtonpost.com/world/national-se_curity/fbi-director-tech-companies-should-be-required-to-make-devi ces-wire-tap-friendly/2014/10/16/93244408-555c-11e4-892e-602188e70e9cstory.html> <<

[11] ROSENSTEIN, Rod J. Deputy Attorney General Rod J. ROSENSTEIN delivers remarks on encryption at the United States Naval Academy. US Department of Justice. (10 de octubre de 2017). <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval> <<

[12] ACHARYA, Bhairav et al. «Deciphering the European encryption debate: United Kingdom». New America (28 de junio de 2017). <https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-united-kingdom> <<

[13] TOOER, Amar. «France and Germany want Europe to crack down on encryption». Verge (24 de agosto de 2016). <https://www.theverge.com/2016/8/24/12621834/france-germany-encryption-terorrism-eu-telegram>. STUPP, Catherine. «Five member states want EU-wide laws on encryption». Euractiv (22 de noviembre de 2016). <https://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption> <<

[14] GIBBS, Samuel. «EU seeks to outlaw ‘backdoors’ in new data privacy proposals». Guardian (19 de junio de 2017). <https://www.theguardian.com/technology/2017/jun/19/eu-outlaw-backdoors-new-data-privacy-proposals-uk-government-encrypted-communications-whatsapp> <<

[15] BAXENDALE, Rachel. «Laws could force companies to unlock encrypted messages of terrorists». Australian (14 de julio de 2017). <http://www.theaustralian.com.au/national-affairs/laws-could-force-companies-to-unlock-encrypted-messages-of-terrorists/news-story/ed481d29c956dfac93610 61a60dcf590> <<

[16] SREEHARSHA, Vinod. «WhatsApp is briefly shut down in Brazil for a third time». New York Times (19 de julio de 2016). <https://www.nytimes.com/2016/07/20/technology/whatsapp-is-briefly-shut-down-in-brazil-for-a-third-time.html> <<

[17] MOON, Mariella. «Egypt has blocked encrypted messaging app Signal». Engadget (20 de diciembre de 2016). <https://www.engadget.com/2016/12/20/egypt-blocks-signal> <<

[18] O'NEILL, Patrick Howell. «Russian bill requires encryption backdoors in all messenger apps». Daily Dot (20 de junio de 2016). <https://www.dailydot.com/layer8/encryption-backdoor-russia-fsb>. Maida, Adam. Online and on all fronts: Russia's assault on freedom of expression. Human Rights Watch (18 de julio de 2017). <https://www.hrw.org/report/2017/07/18/onli ne-and-all-fronts/russias-assault-freedom-expres sion>. Rapoza, Kenneth. «Russia fines cryptocurrency world's preferred mes-saging app, Telegram». Forbes (16 de octubre de 2017). <https://www.forbes.com/sites/kenrapoza/2017/10/16/russia-fines-cryptocurrency-worlds-preferred-messaging-app-telegram> <<

[19] HAAS, Benjamin. «China blocks WhatsApp services as censors tighten grip on internet». Guardian (29 de julio de 2017). <https://www.theguardian.com/technology/2017/jul/19/china-blocks-whatsapp-services-as-censors-tighten-grip-on-internet> <<

[20] LOCLEAR, Mallory. «FBI tried and failed to unlock 7.000 encrypted devices». Engadget (23 de octubre de 2017). <https://www.engadget.com/2017/10/23/fbi-failed-unlock-7-000-encrypted-devices> <<

[21] UPTON, Fred et al. Encryption working group year-end report. House Judiciary Committee and House Energy and Commerce Committee Encryption Working Group, US House of Representatives (20 de diciembre de 2016). <https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf> <<

[22] CANNANE, Steve. «Cracking down on encryption could ‘make it easier for hackers’ to penetrate private services». ABC News Australia (9 de noviembre de 2017). <http://www.abc.net.au/news/2017-11-10/for_mer-mi5-chief-says-encryption-cut-could-lead-to-more-hacking/9136746> <<

[23] NEWMAN, Lily Hay. «Encrypted chat took over. Let’s encrypt calls, too». Wired (21 de abril de 2017). <https://www.wired.com/2017/04/encrypted-chat-took-now-encrypted-callings-turn> <<

[24] DIFFIE, Whitfield; LANDAU, Susan. The export of cryptography in the 20th century and the 21st. Sun Microsystems (1 de octubre de 2001). <https://pdfs.semanticscholar.org/1870/af818dd0075bb5e79764427a7c932fe3cfc6.pdf> <<

[25] British Broadcasting Corporation. «David Cameron says new online data laws needed». BBC News (12 de enero de 2015). <http://www.bbc.com/news/uk-politics-30778424>. Griffin, Andrew. «WhatsApp and Snapchat could be banned under new surveillance plans». Independent (12 de enero de 2015). <https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html> <<

[26] RILEY, Charles. «Theresa May: Internet must be regulated to prevent terrorism». CNN (4 de junio de 2017). <http://money.cnn.com/2017/06/04/technology/social-media-terrorism-extremism-london/index.html> <<

[27] SCHNEIER, Bruce; Seidel, Kathleen; Vijay-akumar, Saranya. «A worldwide survey of encryption products». Publication 20162, Berk man Center for Internet & Society, Harvard University (11 de febrero de 2016). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2731160> <<

[28] DOCTOROW, Cory. «Theresa May wants to ban crypto: Here's what that would cost, and here's why it won't work anyway». Boing Boing (4 de junio de 2017). <https://boingboing.net/2017/06/04/theresa-may-king-canute.html> <<

[29] MOORE, Daniel; Rid, Thomas. «Cryptopolitik and the Darknet». Survival 58, núm. 1 (Febrero de 2016). <https://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085> <<

[30] McConnell, Mike; Chertoff, Michael; Lynn, William. «Why the fear over ubiquitous data encryption is overblown». Washington Post (28 de julio de 2015). <https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html> <<

[31] NISSENBAUM, Helen. «The meaning of anonymity in an information age». Information Society 15 (1 de septiembre de 1998). <http://www.cs.cornell.edu/~shmat/courses/cs5436/meaning-of-anonymity.pdf> <<

[32] El programa de recogida de muestras de la NSA finalizó en 2015. Ahora, las compañías telefónicas guardan los metadatos, y la NSA es capaz de consultar la base de datos bajo petición. Esto supone una pequeña diferencia. SAVAGE, Charlie. «Reined-in NSA still collected 151 million phone records in ’16». New York Times (2 de mayo de 2017). <https://www.nytimes.com/2017/05/02/us/politics/nsa-phone-records.html> <<

[33] CRUMP, Catherine et al. You are being tracked: How license plate readers are being used to record Americans' movements. American Civil Liberties Union (17 de julio de 2013). <https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf> <<

[34] CATE, Fred H.; Dempsey, James X. (eds.). Bulk Collection: Systematic Government Access to Private-Sector Data. Oxford University Press, 2017. <http://www.oxfordscholarship.com/view/10.1093/oso/9780190685515.001.0 9780190685515> <<

[35] GUILLEMIN, Jeanne. «Scientists and the history of biological weapons: A brief historical overview of the development of biological weapons in the twentieth century». EMBO Reports 7 (1 de julio de 2006). <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490304> <<

[36] HARPER, Jim. «The search for answers in Fort Hood». Cato at Liberty (10 de noviembre de 2009). <http://www.cato.org/blog/search-answers-fort-hood>. HARPER, Jim. «Fort Hood: Reaction, response, and rejoinder». Cato at Liberty (11 de noviembre de 2009). <http://www.cato.org/blog/fort-hood-reaction-response-rejoinder> <<

[37] Office of the Inspectors General for the Intelligence Community, Central Intelligence Agency, Department of Justice, and Department of Homeland Security. Summary of information handling and sharing prior to the April 15, 2013 Boston Marathon bombings (10 de abril de 2014; unclassified summary released 6 de diciembre de 2016). <https://www.dni.gov/index.php/who-we-are/organizations/ic-ig/ic-ig-news/1604> <<

[38] LACHOW, Irving. Active cyber defense: A framework for policymakers. Center for a New American Security (22 de febrero de 2013). <https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers> <<

[39] Patrick Lin expone varios de los argumentos muy bien. LIN, Patrick. Ethics of hacking back: Six arguments from armed conflict to zombies. California Polytechnic State University, Ethics + Emerging Sciences Group (26 de septiembre de 2016). <http://ethics.calpoly.edu/hackingback.pdf> <<

[40] WOLFF, Josephine. «Attack of the hack back». Slate (17 de octubre de 2017). <http://www.slate.com/articles/technology/future_tense/2017/10/hacking_bacl <<

[41] WOLFF, Josephine. «When companies get hacked, should they be allowed to hack back?». Atlantic (14 de julio de 2017). <https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679> <<

[42] ROBERTSON, Jordan; RILEY, Michael. «Would the U.S. really crack down on companies that hack back?». Bloomberg (30 de diciembre de 2013). <https://www.bloomberg.com/news/2014-12-30/why-would-the-u-s-crack-down-on-companies-that-hack-back-.html> <<

[43] GRAVES, Tom. Rep. Tom GRAVES formally introduces active cyber defense bill (13 de octubre de 2017). <https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=398840> <<

[44] BAKER, Stewart A. The attribution revolution: Raising the costs for hackers and their customers: Statement of Stewart A. Baker, Partner, Steptoe & Johnson LLP, before the Judiciary Committee's Subcommittee on Crime and Terrorism, United States Senate (8 de mayo de 2013). <https://www.judiciary.senate.gov/imo/media/doc/5-8-13BakerTestimony.pdf>. Baker, Stewart A. Testimony of Stewart A. Baker before the Committee on Homeland Security and Governmental Affairs, United States Senate: The Department of Homeland Security at 10 Years: Examining Challenges and Addressing Emerging Threats (11 de septiembre de 2013). <https://www.hsgac.senate.gov/hearings/the-department-of-homeland-security-at-10-years-examining-challenges-and-achievements-and-addressing-emerging-threats>. Baker, Stewart A.; Kerr, Orin; Volokh, Eugene. «The hackback debate». Steptoe Cyberblog (2 de noviembre de 2012). <https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate>. BAKER, Stewart A. «The case for limited hackback rights». Washington Post (22 de julio de 2016). <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/22/the-case-for-limited-hackback-rights> <<

[45] FINOCCHIARO, Charles. «Personal factory or catalyst for piracy? The hype, hysteria, and hard realities of consumer 3-D printing». Cardozo Arts and Entertainment Law Journal 31 (18 de marzo de 2013). <http://www.cardozoaelj.com/issues/archive/2012-13>. Susson, Matthew Adam. Watch the world 'burn': Copyright, micropatent and the emergence of 3D printing (Abril de 2013). Chapman University School of Law. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2253109> <<

[46] DOCTOROW, Cory. «Lockdown: The coming war on general-purpose computing». Boing Boing (10 de enero de 2012). <http://boingboing.net/2012/01/10/lockdown.html>. DOCTOROW, Cory. «The coming civil war over general purpose computing». Boing Boing (23 de agosto de 2012). <http://boingboing.net/2012/08/23/civilwar.html> <<

[47] WOYACH, Kristen Ann et al. «Crime and punishment for cognitive radios». 2008 46th Annual Allerton Conference on Communication, Control, and Computing (23-26 de septiembre de 2008). <http://ieeexplore.ieee.org/document/4797562> <<

[1] Hay mucho más sobre esta tendencia que va más allá del alcance de este libro. TWENGE, Jean M.; CAMPBELL, W. Keith; CARTER, Nathan T. «Declines in trust in others and confidence in institutions among American adults and late adolescents, 1972-2012». *Psychological Science* 25, núm. 10 (9 de septiembre de 2014). <http://journals.sagepub.com/doi/abs/10.1177/0956797614545133>.
HALPERN, David. *Social trust is one of the most important measures that most people have never heard of and it's moving*. Behavioural Insights Team (12 de noviembre de 2015). <http://www.behaviouralinsights.co.uk/uncategorized/social-trust-is-one-of-the-most-important-measures-that-most-people-have-never-heard-of-and-its-moving>. GOULD, Eric D.; HIJZEN, Alexander. «Growing apart, losing trust? The impact of inequality on social capital». *International Monetary Fund Working Paper* núm. 16/176 (22 de agosto de 2016). <https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Growing-Apart-Losing-Trust-The-Impact-of-Inequality-on-Social-Capital-44197>.
D'OLIMPIO, Laura. «Fear, trust, and the social contract: What's lost in a society on permanent alert». *ABC News* (25 de octubre de 2016). <http://www.abc.net.au/news/2016-10-26/fear-trust--social-contract-society-on-permanent-alert/7959304> <<

[2] OLMSTEAD, Kenneth. Most Americans think the government could be monitoring their phone calls and emails . Pew Research Center (27 de septiembre de 2017). <http://www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-government-could-be-monitoring-their-phone-calls-and-emails> <<

[3] DONILON, Thomas E. et al. *Report on securing and growing the digital economy*. Commission on Enhancing National Cybersecurity (1 de diciembre de 2016). <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf> <<

[4] SCHNEIER, Bruce. Liars and Outliers: Enabling the Trust That Society Needs to Thrive. Wiley, 2012. <http://www.wiley.com/WileyCDA/WileyTitle/productCd1118143302.html> <<

[5] HWANG, Tim; Kamdar, Adi. «The theory of peak advertising and the future of the web», version 1. Working Paper, Nesson Center for Internet Geophysics (9 de octubre de 2013). < http://peakads.org/images/Peak_Ads.pdf> <<

[6] PERROW, Charles. Normal Accidents: Living with High-Risk Technologies. Princeton University Press, 1999. <https://www.amazon.com/Normal-Accidents-Living-High-Risk-Technologies/dp/0691004129>. PERROW, Charles. «Organizing to reduce the vulnerabilities of complexity». Journal of Contingencies and Crisis Management 7, núm. 3 (1 de septiembre de 1999). <http://onlinelibrary.wiley.com/doi/10.1111/1468-5973.00108/full> <<

[7] WILDAVSKY, Aaron B. Searching for Safety. Transaction Publishers, 1988. <https://books.google.com/books?id=rp6U8JsPlM0C> <<

[8] SCHNEIER, Bruce. «Resilient security and the Internet». ICANN Community Meeting on Security and Stability of the Internet Naming and Address Allocation Systems, Los Angeles, California (14 de noviembre de 2001).
<http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/schneier.html>.
Black Hat. «Speakers». Black Hat Briefings ’01, July 11-12, Las Vegas.
<https://www.blackhat.com/html/bh-usa-01/bh-usa-01-speakers.html>
[Consulta 24 abril 2018] <<

[9] SCHNEIER, Bruce. Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Springer, 2006. <https://books.google.com/books?id=btgLBwAAQBAJ&pg=PA120> <<

[10] World Economic Forum. Risk and responsibility in a hyperconnected world: Pathways to global cyber resilience (7 de junio de 2012). <https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience> <<

[11] TREVERTON, Gregory et al. Global trends: Paradox of progress, NIC 2017-001. National Intelligence Council. <https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf> <<

[12] HEALEY, Jason. Building a defensible cyberspace: Report of the New York Cyber Task Force. Columbia School of International and Public Affairs (28 de septiembre de 2017). <http://globalpolicy.columbia.edu/sites/default/files/nyctf_2017-09-28_report.pdf> <<

[13] HEALEY, Jason; Pitts, Hannah. «Applying international envi ronmental legal norms to cyber statecraft». I/S: A Journal of Law and Po licy for the Information Society 8, núm. 2 (1 de octubre de 2012). <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/6.Healey.Pitts_.pdf <<

[14] SHACKELFORD, SCOTT J. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace . Cambridge University Press, 2016. <https://books.google.com/books/?id=_q2BAwAAQBAJ> <<

[15] ROFF, Heather M. Cyber peace: Cybersecurity through the lens of positive peace. New America Foundation (24 de febrero de 2016). <https://static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf> <<

[1] GEER, Dan. «Measuring security». *USENIX Security Symposium* (6 de agosto de 2007). <http://geer.tinho.net/measuringsecurity.tutorial.pdf> <<

[2] El economista Tim Harford ha señalado esto recientemente. Harford, Tim. «What we get wrong about technology». FT Magazine (8 de julio de 2017). <http://timharford.com/2017/08/what-we-get-wrong-about-technology> <<

[3] Esta ley fue inventada por Roy Amara, experto informático de la Universidad de Staford, que también dirige el Instituto para el Futuro. Ridley, Matt. «Amara's law». Matt Ridley Online (12 de noviembre de 2017). <http://www.rationaloptimist.com/blog/amaras-law> <<

[4] SCHNEIER, Bruce. «Artificial intelligence and the attack/defense balance». IEEE Security & Privacy (Marzo abril de 2018). <https://www.schneier.com/essays/archives/2018/03/artificial_intellige.html> <<

[5] Wikiquote. Otto von Bismarck. <https://en.wikiquote.org/wiki/Otto_von_Bismarck> [Consulta 8 mayo 2018] <<

[6] BOHM, Nicholas; Brown, Ian; Gladman, Brian. «Electronic commerce: Who carries the risk of fraud?». Journal of Information, Law & Technology 2000, núm. 3 (31 de octubre de 2000). <http://www.ernest.net/writing/FraudRiskAllocation.pdf> <<

[7] ILVES, Toomas Hendrik. Rebooting trust? Freedom vs. security in cyberspace. Office of the President, Republic of Estonia (31 de enero de 2014). <https://vp2006-2016.president.ee/en/official-duties/speeches/9796-qrebooting-trust-freedom-vs-security-in-cyberspaceq> <<

[8] TITCOMB, James. «Malcolm Turnbull says laws of Australia trump laws of mathematics as tech giants told to hand over encrypted messages». Telegraph (14 de julio de 2017). <http://www.telegraph.co.uk/technology/2017/07/14/malcolm-turnbull-says-laws-australia-trump-laws-mathematics> <<

[9] Aquí, SWEENEY describe la investigación que llevó a la anonimización de los datos médicos que pertenecían a William Weld, entonces gobernador de Massachusetts: SWEENEY, Latanya.computational disclosure control: A primer on data privacy protection (8 de enero de 2001). <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf> <<

[10] Aquí hay un documento: SWEENEY, Latanya. «Discrimination in online ad delivery» communications of the Association of Computing Machinery 56, núm. 5 (Enero de 2013). <https://arxiv.org/abs/1301.6822> <<

[11] SWEENEY, Latanya. «k-Anonymity: A model for protecting privacy». International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems 10, núm. 5 (2002). <https://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.html <<

[12] Este es su último libro: LANDAU, Susan. Listening In: Cybersecurity in an Insecure Age, Yale University Press, 2017. <https://books.google.com/books?id=QZ47DwAAQBAJ> <<

[13] Esta es su última declaración: LANDAU, Susan. Testimony for House Judiciary Committee hearing on 'The encryption tightrope: Balancing Americans' security and privacy' (1 de marzo de 2016). <https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf> <<

[14] Aquí hay un documento: Feldman, Ariel; Halderman, J. Alex; Felten, Edward W. «Security analysis of the Diebold AccuVote-TS voting machine». 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (13 de septiembre de 2006). <https://citp.princeton.edu/research/voting> <<

[15] American Civil Liberties Union. About the ACLU's Project on Speech, Privacy, and Technology. <https://www.aclu.org/other/about-aclus-project-speech-privacy-and-technology> [Consulta 24 abril 2018] <<

[16] Aquí puedes encontrar una discusión sobre el tema y una buena lista de programas: Davidson, Alan; WHITE, Maria; Fiorille, Alex. Building the future: Educating tomorrow's leaders in an era of rapid technological change. New America/Freedman Consulting (26 de febrero de 2018) <<

[17] Internet Policy Research Initiative. Massachusetts Institute of Technology. <https://internetpolicy.mit.edu> [Consulta 24 marzo 2018] <<

[18] Georgetown Law. Center on Privacy & Technology. <https://www.law.georgetown.edu/academics/centers-institutes/privacy-technology> [Consulta 24 abril 2018] <<

[19] Digital HKS. Harvard Kennedy School. <https://projects.iq.harvard.edu/digitalhks/home> [Consulta 24 abril 2018] <<

[20] NetGain es un consorcio de grandes fundaciones que tratan de hacer que esto suceda. Freedman, Tom et al. A pivotal moment: Developing a new generation of technologists for the public interest. NetGain Partnership (10 de febrero de 2016). <https://www.netgainpartnership.org/resources/2018/1/26/a-pivotal-moment> <<

[21] Freedman Consulting. Here to there: Lessons from public interest law unpublished memo (3 de marzo de 2006) <<

[22] GRAHAM, Robert L. «Balancing the scales of justice: Financing public interest law in America». Loyola University Chicago Law Journal 8, núm. 3 (1977). <http://lawecommons.luc.edu/luclj/vol8/iss3/10> <<

[23] NIELSEN, Laura Beth; Albiston, Catherine R. «The organization of public interest practice: 1975-2004». North Carolina Law Review 84 (1 de enero de 2005). <http://scholarship.law.berkeley.edu/facpubs/1618> <<

[24] De hecho, algunos creen que esta cifra es lamentablemente baja. Davis, Pete. «Our bicentennial crisis: A call to action for Harvard Law School's public interest mission». Harvard Law Record (26 de octubre de 2017). <http://hlrecord.org/wp-content/uploads/2017/10/OurBicentennialCrisis.pdf> <<