BRUCE SCHNEIER

ESTE EXPERTO EN CIFRADO Y ALGORITMOS ES TAN CONOCIDO QUE SU FAMA LLEGA A HOLLYWOOD. CONSIDERA QUE EL MUNDO ACTUAL ES SEGURO... PERO QUE CORREMOS DEMASIADOS RIESGOS. Y, POR ESO, PIDE A LOS POLÍTICOS MAYOR IMPLICACIÓN. #Texto: José M. Vera

Le obsesiona que estemos conectando a Internet todo lo que nos rodea: desde móviles hasta coches e, incluso, ciudades. Y que la prisa por conseguirlo nos lleve a hacerlo de manera poco segura. Bruce Schneier, experto en proteger la información con potentes algoritmos de cifrado, es uno de esos tipos nunca te dejan indiferentes. Por algo es uno de los ciberexpertos más citados en las películas de Hollywood. Con este perfil, es lógico que su presencia no pasara desapercibida en su intervención en la **Jornada Internacional de Seguridad de la Información del ISMS Forum**, en Madrid.

¿Cómo te defines?

Como un tecnólogo de la seguridad: trabajo en la intersección entre las tecnologías de seguridad y cómo las aplica la gente.

¿Qué es para ti estar seguro en la actualidad?

Si estás vivo, estás en riesgo. Si estás muerto estás seguro. Partiendo de este punto, es cierto que el grado de seguridad varía según quién eres, qué haces o quién querría escucharte. Estar seguro es reducir el riesgo de cualquier amenaza. ¿Eres del gobierno de los EE.UU., del gobierno chino, un ejecutivo, un criminal, un terrorista? Depende de todas esas cosas.

> "Sale más barato diseñar objetos seguros desde el principio... que arreglar los que no lo son"

¿Por qué está cambiando el mundo?

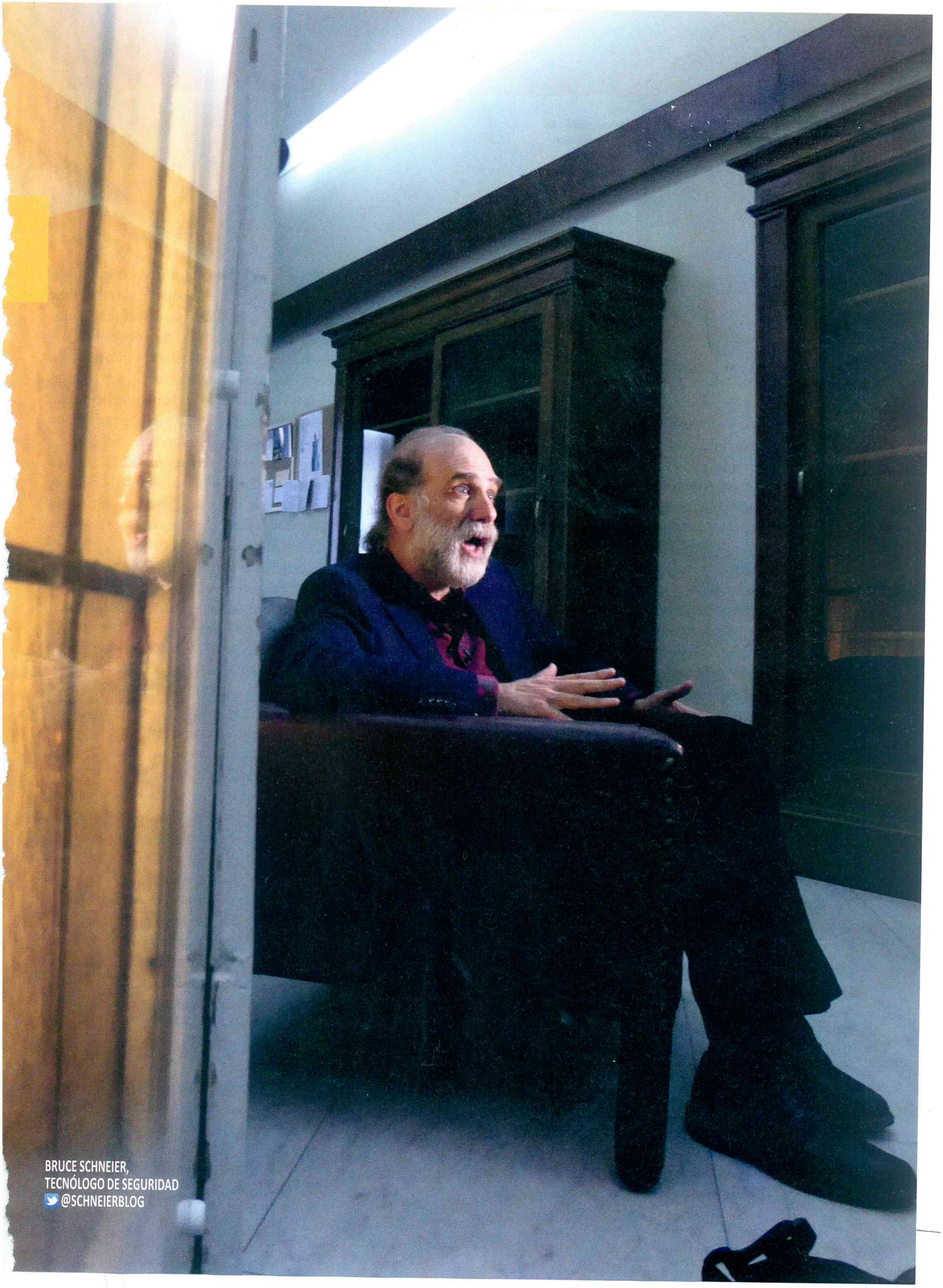
Hemos convertido en ordenadores a teléfonos, juguetes, electrodomésticos... Así que los problemas que sufrimos con los ordenadores... se van a trasladar a todo lo demás. Eso es lo que trae el Internet de las Cosas -IoT- y por eso es importante asegurarnos que todos estos dispositivos que ahora conectamos sean seguros y no incluyan vulnerabilidades heredadas.

¿Qué hay que tener en cuenta...?

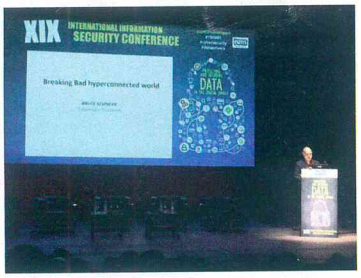
Que ya vivimos en un mundo hiperconectado. Todo lo que nos rodea comunica datos, desde un termostato hasta un coche. Unos datos que son recogidos y enviados por sensores. Así que se puede considerar a los sensores como los pies de internet y lo que está en medio es el cerebro. Estamos creando un internet que piensa, siente y actúa. ¿Te suena? Sí, es la definición de un robot.

¿Qué es lo que más te preocupa?

La falta de privacidad. Se trata de una amenaza mundial, pero



BRUCE SCHNEIER,
TECNÓLOGO DE SEGURIDAD
@SCHNEIERBLOG



Schneier pidió a los gobiernos mayor regulación en la fabricación y diseño de todo tipo de dispositivos conectados en su charla en la XVIII Jornada Internacional de Seguridad de la Información del ISMS Forum.

también es un reto. Estamos acostumbrados a la confidencialidad, a la protección y a tener el control de nuestros datos. Pero ahora en este mundo perdemos ese poder. La información está cada vez más amenazada por la manipulación.

¿Por qué todo parece tan mal hecho?

Cuando hablamos de amenazas pensamos en ordenadores o teléfonos, pero lo cierto es que tienen los mismos sistemas que un avión, así que los aparatos en sí son seguros. El gran problema es que la mayor parte del software que se utiliza tiene fallos de seguridad. Y no queremos pagar por software de alta calidad: primamos lo barato y rápido en vez de lo bueno y caro. Y eso facilita los ataques.

Qué te preocupa del mundo cibernético

Los sistemas que, siendo 'cíber', afectan al mundo físico. Creo que no estamos preparados para un ciberataque que tenga consecuencias.

La primera enseñanza 'cíber' que aprendiste... Que la seguridad absoluta no existe. Y que nada es gratuito: cuanta más seguridad tienes... más renuncias a otras cosas, ya sea a dinero, comodidades... Hay que buscar un punto que beneficie a todos.

Y lo último... Que nunca se sabe lo suficiente.

Eres experto en algoritmos, ¿por qué son importantes?

Un algoritmo es lista ordenada de instrucciones para solucionar un problema matemático o informático. Por eso, cuando los escribimos debemos ser cuidadosos para que sean seguros. Eso sí, sirven para todo. Hay algoritmos que toman decisiones y determinan quién sale y quién no de la cárcel, quién entra en la universidad o a qué servicios tienes derecho en un hospital.

Tus sistemas de cifrado son imposibles de romper... De momento sí, pero hay que pensar que llegará la computación cuántica y lo cambiará todo. Y me preocupa cómo se aplicará.

SU 'FÓRMULA' DE LA CIBERSEGURIDAD

01 Conectividad. Hay sistemas que son seguros desde su diseño, pero cuando se conectan -a veces a dispositivos que no lo son- ... dejan de serlo. Es un tema complicado de arreglar, pero hay que conseguirlo.

02 Normativa: Hay que hacer normas que obliguen a vender productos seguros. Los gobiernos tienen que implicarse cada vez más.

03 Diseño: Hay que hacer las cosas seguras desde su diseño inicial. También que ser ágiles y actualizar rápido el software.

04 Punto de equilibrio: Hay que escoger entre el coste de evitar el fallo haciendo las cosas seguras... y el de arreglarlas cuando han sido vulneradas. Y es vital desarrollar todo rápido y bien: dos formas que, hasta ahora, eran antagónicas.

05 Sanciones: Poco motiva tanto como el miedo. También hay que imponer sanciones a los que no hagan cosas seguras.

Te sientes orgulloso... ¡De mis algoritmos criptográficos! Sobre todo de Twofish, que es el que más trabajo me ha llevado, pero también el de Blowfish o Fortuna. Todos tienen muchas aplicaciones, según lo que necesites. Por ejemplo, son muy importantes para cifrar la información y que nadie, excepto tú, acceda a ella. Por eso son importantes. También estoy orgulloso de los libros que he escrito, porque creo que explican bien la tecnología a gente que no está familiarizada, y eso me parece algo fundamental.

¿Te gusta vivir en un mundo conectado? Sí, porque sus beneficios son increíbles y porque no me imagino volviendo a un mundo desconectado. La pregunta es, ¿ahora, cómo lo hacemos seguro?

¿Confías en las máquinas inteligentes? Sí, porque no nos queda otra. Todos dependemos ya de muchas máquinas lo queramos o no.

Algunos consideran que la Inteligencia Artificial será un peligro...

Sí, pero como casi todo. La misma tecnología tiene una cara buena y una mala. Depende de cómo se utilice.

¿Podría producirse un 'Pearl Harbor cibernético'?

Todos los ataques son posibles pero también lo son las formas de defendernos de esos ataques. ¿Estás a salvo de ser asesinado? No. Pero vives haciendo las cosas necesarias para evitarlo.

¿Viviremos ciberseguros algún día?

No lo creo, por lo menos durante un tiempo. Avanzamos a trompicones. De momento lo importante es hacer una lista de buenas prácticas y que la gente las ponga en marcha cuanto antes.

¿Qué consejo le darías a las autoridades responsables de la ciberseguridad en España?

Que sigan apostando por aplicar las normas que permitan hacer un mundo ciberseguro tanto por parte de España como por la UE. Me parecen fantásticas muchas de las que se han aprobado, como la Estrategia de Ciberseguridad Nacional.