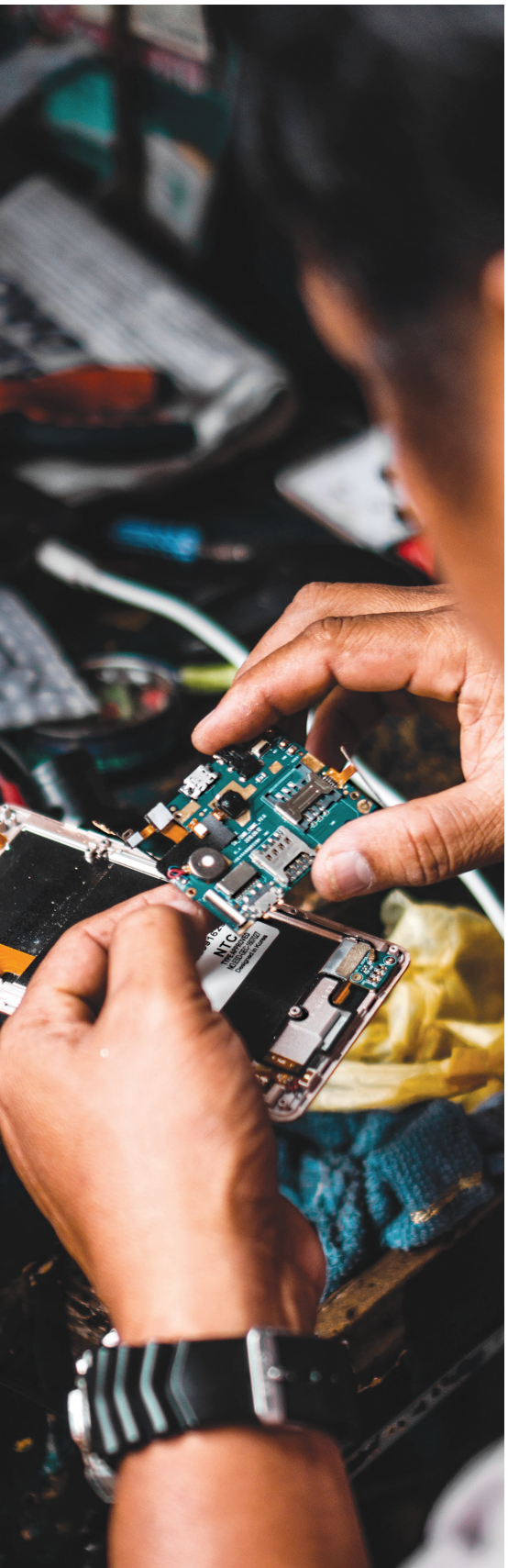

LA INDUSTRIA DE LA INSEGURIDAD

Edward Snowden
Traducción de Mir Rodríguez Lombardo

Cuando llega a mis manos un teléfono nuevo, lo primero que hago es desarmarlo. No porque tenga la afición de inspeccionar aparatos ni por mis principios políticos, sino por el riesgo que conlleva usarlo. La reparación del hardware, que consiste en extraer quirúrgicamente los dos o tres micrófonos diminutos que tiene en su interior el teléfono, es sólo el principio de un proceso arduo. Incluso tras varios días de mejoras de seguridad hechas de manera artesanal, mi teléfono inteligente seguirá siendo el artículo más peligroso que poseo.

Antes de la publicación del "Proyecto Pegasus", la mayoría de los fabricantes de teléfonos inteligentes y buena parte de la prensa suspiraban de hastío cada vez que yo afirmaba públicamente que un iPhone recién sacado de la caja es una amenaza letal en potencia. Pegasus es un trabajo periodístico de varios medios importantes alrededor del mundo dirigido a revelar las consecuencias fatales de las actividades del Grupo NSO, el nuevo rostro empresarial de una industria de la inseguridad fuera de control.

Muchos se resisten a aceptar que algo que te trae placer no necesariamente es bueno, sin importar los años de investigación que conectaban al negocio de hackeo telefónico del Grupo NSO con las muertes y detenciones de periodistas y defensores de los derechos humanos; sin importar los años de investigación que confirman que los sistemas operativos de los teléfonos inteligentes están llenos de problemas de seguridad catastróficos (empeorados a su vez por un código escrito en lenguajes

◂ Un teléfono celular desarmado. Fotografía de Clint Bustrillos ©

de programación antiguos que, ya sabemos, son inseguros) y a pesar de los años de investigación que apuntan que, incluso cuando todo funciona correctamente, el ecosistema móvil es un infierno distópico de monitoreo y manipulación de los usuarios.

El "Proyecto Pegasus" es un punto de quiebre: un reportaje bien investigado, con fuentes exhaustivas, que relata una historia francamente desquiciada sobre una infección causada por un "caballo de Troya con alas" llamado "Pegasus" que básicamente transforma el teléfono en tu bolsillo en un dispositivo de seguimiento todopoderoso que puede encenderse y apagarse, remotamente, sin que tú, el dueño del bolsillo, te enteres de nada.

Según lo describe el *Washington Post*:

> Pegasus puede recabar correos electrónicos, registros de llamadas, publicaciones en redes sociales, contraseñas de usuario, listas de contactos, imágenes, videos, grabaciones de sonido e historiales de navegación; puede activar cámaras o micrófonos para capturar nuevas imágenes y grabaciones. Puede escuchar llamadas y correos de voz. Puede recopilar datos de ubicación de dónde ha estado un usuario y además determinar dónde está ese usuario en este instante, junto con datos que indican si la persona está inmóvil o, en caso contrario, en qué dirección se está desplazando.

El teléfono que tienes en la mano opera en un estado de inseguridad permanente, abierto a infecciones cortesía de cualquiera que esté dispuesto a poner dinero en la mano de esta nueva Industria de la Inseguridad. La totalidad del negocio de esta Industria implica conjurar nuevos tipos de infección (capaces de eludir las más recientes vacunas digitales) y venderlos.

Una Industria de esta naturaleza, cuyo único fin es la producción de vulnerabilidad, debe ser desmantelada.

2.

Incluso si mañana despertáramos y un volcán con conciencia ciudadana hubiera borrado por completo a todo el Grupo NSO y a los empresarios privados de su calaña, la realidad seguiría siendo que estamos en medio de la mayor crisis de seguridad informática en la historia de la computación. Los que se dedican a crear el software que está detrás de los dispositivos electrónicos de los que nos valemos se conforman con escribir código en lenguajes de programación que sabemos que son inseguros porque, pues, eso es lo que siempre han hecho, y la modernización requiere un esfuerzo importante. La gran mayoría de las vulnerabilidades que son descubiertas y explotadas por la Industria de la Inseguridad se generan por razones técnicas, relacionadas con la manera en que una computadora lleva un control de lo que supuestamente está haciendo en el momento exacto en que el código se escribe, lo que hace que la elección de un lenguaje más seguro sea una protección crucial... y sin embargo es algo que pocos practican.

Si queremos ver un cambio, hace falta incentivarlo. Por ejemplo: si quieres que a Microsoft le dé un infarto, hablemos de la idea de definir responsabilidades legales por código defectuoso en un producto comercial. Si le quieres dar pesadillas a Facebook, hablemos de la idea de hacerlos legalmente responsables de todas y cada una de las filtraciones de nuestros datos personales que se pueda comprobar que fueron capturados innecesariamente. Imagínate la velocidad a la que Mark Zuckerberg empezaría a martillar la tecla "suprimir".

Diferentes modelos de teléfonos celulares. Fotografía de Eirik Solheim ©

3.

El hackeo patrocinado por el Estado se ha vuelto una carrera tan habitual que debería tener su propia categoría olímpica en Tokio 2020. Cada país califica de criminales las actividades del otro, mientras que se rehúsa a reconocer la culpa de sus propias infracciones.

Si el hackeo no es ilegal cuando nosotros lo hacemos, no hay manera de que sea ilegal cuando lo hacen los otros, y resulta que ese "otros" se refiere cada vez más al sector privado. Aquí hay un principio básico del capitalismo: es cuestión de negocios. Si todo el mundo lo está haciendo, ¿por qué yo no?

Recordemos nuestro tema anterior sobre el Pegasus del Grupo NSO, que especial pero no exclusivamente ataca a los iPhones. Si bien los iPhones son de por sí más privados y en algunos casos están mejor diseñados desde el punto de vista de seguridad, también son como un monocultivo: si encuentras la manera de infectar uno, podrás (probablemente) infectarlos a todos, un problema exacerbado por la política de Apple, que cierra toda posibilidad a los usuarios de hacer modificaciones a la manera en que operan los dispositivos iOS. Cuando se combina este monocultivo y la política de caja negra con la popularidad casi universal de Apple entre la élite global, queda clara la razón por la que el Grupo NSO tiene una fijación con el iPhone.

Nos guste o no, enemigos y aliados comparten un entorno común, y cada día nos volvemos más dependientes de dispositivos que emplean un código común.

No permitimos un mercado de servicios de infecciones biológicas: lo mismo debe valer para las infecciones digitales.

4.

En tecnología, igual que en salud pública, para proteger a uno tenemos que protegerlos a todos. El primer paso en esta dirección, o al menos el primer paso digital, debe ser prohibir el comercio de software de intrusión. No permitimos un mercado de servicios de infecciones biológicas: lo mismo debe valer para las infecciones digitales. Eliminar el ánimo de lucro reduce el riesgo de proliferación a la vez que asegura el desarrollo tecnológico, dejando espacio para la investigación con fines públicos y las labores inherentes al gobierno.

Aunque retirar el software de intrusión del mercado comercial no se lo quita también a los Estados, sí asegura que algún narcotraficante o criminal sexual de Hollywood que pueda sacar unos cuantos millones de abajo del colchón no pueda infectar todos los iPhones del planeta.

Una moratoria de esa naturaleza, sin embargo, sólo sirve para comprar tiempo. Después de la prohibición, el paso siguiente es asignar responsabilidad legal. Es esencial que entendamos que ni la escala del negocio del Grupo NSO ni las consecuencias que ha infligido a la sociedad global serían posibles sin el acceso al capital global de empresas amorales, como Novalpina Capital (Europa) y Francisco Partners (EE. UU.) La consigna es simple: o desinvierten sus fondos, o sus propietarios serán detenidos. El único producto de esta industria es el daño intencional y previsible, por lo que estas empresas inversionistas son cómplices voluntarias.

5.

Imagina que eres el consejero editorial del *Washington Post* (primero tendrías que deshacerte de tu integridad). Imagina que a tu columnista lo asesinan y que respondes con una solicitud en la que susurras a los autores del asesinato que la próxima vez, por favor, deben llenar unos cuantos formularios adicionales. Francamente, la respuesta del *Post* al escándalo del NSO es tan vergonzosamente débil que es un escándalo por sí misma: ¿cuántos de sus escritores necesitan morir para que se den cuenta de que los procesos no reemplazan a la prohibición?

Con "Pegasus", Arabia Saudita hackeó los teléfonos de la exesposa de Yamal Jashogyi y de su prometida, y usó la información extraída para prepararse rumbo a su monstruoso asesinato y su posterior encubrimiento.

El "producto" (léase: "servicio criminal") del Grupo NSO ha sido utilizado para espiar a muchos otros periodistas, jueces e incluso profesores; a candidatos de la oposición, a los cónyuges e hijos de sus objetivos, a sus médicos, a sus abogados e incluso a sus sacerdotes. Esto es lo que aquellos que piensan que una prohibición es "demasiado extrema" no parecen entender: lo que esta industria vende es la oportunidad de acribillar a balazos en el autolavado a los periodistas que no te agradan.

Si no hacemos nada para detener la venta de esta tecnología, no sólo van a ser 50 mil personas en la lista de objetivos: van a ser 50 millones de personas, y pasará mucho más rápido de lo que imaginamos.

Así se verá el futuro: un mundo de personas tan entretenidas con sus teléfonos que no se dan cuenta de que otro es el que los controla. U

Selección del artículo publicado en *Continuing Ed- with Edward Snowden* el 26 de julio del 2021. Disponible en https://edwardsnowden.substack.com/p/ns-oh-god-how-is-this-legal