Alejandro Suárez Sánchez-Ocaña

Autor del libro 'El quinto elemento'. Empresario del sector de internet desde 1996, fue de los primeros en poner a Google bajo el foco con su anterior título, 'Desnudando a Google'. Ayer presentó en Palma 'El quinto elemento', en el que habla sobre espionaje en la red y ciberguerra. Revela cosas como que los servicios secretos usan *apps* como Angry Birds para recabar datos personales o cómo usará ISIS la tecnología para seguir atentando.

"Los servicios secretos prohíben a Obama usar iPhone por seguridad. En España damos uno a cada diputado". M.M.SIERRA

"El próximo gran atentado yihadista será tecnológico y en pocos años: ya están ensayando"

Mar Ferragut
PALMA

FOTO DE **MARIA DEL MAR SIERRA**

— "La realidad que te están ocultando: el próximo 11S empezará con un clic". ¿Es una frase que queda bien para poner en la portada y vender libros o tan grave es el asunto?

— Es un hecho. Los terroristas están usando la tecnología para comunicarse, como por ejemplo han hecho en París, y provocar atentados pero a medio medio plazo la usarán no como medio sino como fin. Empieza a tener poco sentido un tío con un Kalashnikov pegando tiros en París, porque un tío en las montañas de Pakistán con un ordenador puede hacer saltar por los aires una central nuclear, dominar el sistema de control de aguas o cambiar los raíles de todo el sistema ferroviario de un país.

Son nuevos atentados y que ya se están ensayando para poder hacerlos en pocos años. Si hay gente dispuesta a hacer todo tipo de barbaridades como inmolarse, aún más dispuestos estarán a utilizar así la tecnología. Habrá un gran atentado tecnológico en los próximos años y será entonces cuando creemos una industria para intentar evitar que eso vuelva a suceder. Así pasó con el 11S con las medidas de seguridad en los aeropuertos. Ahora pasará lo mismo. Cuando ocurra algo, y va a ocurrir porque ya lo están ensayando, se pondrá en marcha una industria para minimizar el mal uso de la tecnología.

— ¿Vamos a rebufo entonces?

— Sí, porque ahora no hay demanda. Los fabricantes de drones los fabrican a toda mecha porque hay una demanda brutal, pero la tecnología para inhibir esos drones no se fabrica porque aún no se demanda. Cuando ocurra algo y haya un atentado con drones, como ha alertado ahora el ministro italiano de un posible atentado del ISIS con drones en Roma, el dinero público se pondrá al servicio de la industria para buscar soluciones a ese problema.

— Anonymous dice que ha declarado la guerra a ISIS, ¿significa eso algo?

— Es un mensaje más de cara a la galería. Anonymous es una agrupación no reglada de mucha gente, cada uno piensa distinto, y no actúan siempre bajo un mismo criterio. Es muy difícil declararle la guerra a alguien que no necesita la tecnología para vivir. Si declaras la guerra a un país, pues la bolsa, el control de armas, la energía... todo depende de la tecnología, ahí tienes una oportunidad de hacer daño; pero a estos tipos del ISIS que viven con un caballo en la mitad de Siria solo les puedes *hackear* las cuentas de Twitter. Pero si les cierras 500 cuentas, al día siguiente han abierto 800 nuevas con robots automatizados. No necesitan la tecnología en el día a día, nosotros sí. Ellos tienen donde golpear, pero nosotros no, más allá de un punto de vista militar tradicional. ISIS no tiene bancos a los que puedas acceder vía informática.

— ¿Enfrentarse a la ciberguerra es poner puertas al campo?

— Con la tecnología actual es muy difícil. Vivimos en una felicidad irreal y en una libertad vigilada en la que no somos conscientes de todo lo que la tecnología puede hacer en nuestra contra. Hoy es muy difícil de contrarrestar un posible ataque así. En España hay unas 8.000 estructuras críticas –centrales eléctricas, del sistema financiero... – a proteger.

— ¿Está España preparada?

— Falta mucho presupuesto y mucha cultura de la ciberseguridad, ya que aún no ha pasado nada gordo. En el Centro Criptológico Nacional de León trabajan las 220 personas encargadas de proteger esas 8.000 estructuras. El Ejército de EEUU tiene para esto 60.000 personas. Aunque tienen también muchas más estructuras críticas, en esto son cabeza de león.

— ¿Ése señor en la montaña de Pakistán, el ISIS, tiene nivel tecnológico para acometer estos atentados?

— Están aprendiendo. El problema es que aquí tenemos un déficit enorme de talento informático. Tras los atentados de París el CNI se ha lanzado a contratar personas del este de Europa como hackers. La ciberseguridad es una formación no reglada que va a crecer exponencialmente. En Europa del este hay mucho matemático e ingeniero experto en estas cosas, por eso se pesca mucho ahí, para lo bueno y para lo malo: las organizaciones criminales también se surten de ahí.

— En el libro explica que el CNI compra virus troyanos espías ¿Con quién los usan?

— Con nosotros, los usuarios.

— El comentario del ciudadano medio: ¿A quién le importan mis datos, dónde como o a quién llamo?

— Hay ahí dos cosas. Primero: los datos son preventivos. Si yo tengo la capacidad tecnológica para monitorizar y grabar todo por si algún día lo necesito, pues lo hago, y si algún día lo necesito ya lo tengo. Hablamos de grabaciones masivas independientemente de quien sea el *target*. La Agencia de Seguridad de los EEUU (la NSA) ya en los 90 grababa dos mil millones de conversaciones telefónicas diarias, aleatorias. Luego está el espionaje a medida. La NSA, o quien sea, decide que tu teléfono móvil es sensible, pero quizás no por ti, sino por alguien con quien tu te comunicas o el sitio donde trabajas. Tu puedes ser la puerta a los sistemas de otra persona o empresa. Y también muchas veces te espían no por quién eres ahora, sino por quién puedes llegar a ser. La NSA estuvo grabando durante años a Angela Merkel antes de que llegara a canciller. Es prevención. Hay mucha gente con capacidad decisoria y económica susceptible de ser grabada. Y si tiene un hijo, por el que es más fácil acceder, pues también se le graba.

— ¿Nadie está a salvo?

— Estamos a salvo de las amenzas más rudas y evidentes, pero de las más sofisticadas nadie está a salvo. Ningún móvil, ningún *tablet* ni ningún ordenador puede librarse y quien cree que un antivirus le protege es que no entiende lo que ocurre. Estas herramientas usan *zero days,* que son agujeros de seguridad que ni siquiera conocen los fabricantes del softwate y valen millones de euros en el mercado negro. Los compran desde terroristas hasta agencias de investigación de determinados países. Les sirve para grabar todo, monitorizar e introducir lo que deseen en tus sistema.

— ¿Con la tecnología adecuada cualquiera puede dejar un documento comprometedor e ilegal en tus dispositivos?

— Sí. De hecho ésa es una de las funcionalidades del software de Hacking Team que tiene el CNI, como se filtró cuando saltó el escándalo este verano. Si no he encontrado ninguna prueba aunque tenga la certeza de que eres culpable, la puedo fabricar a medida. La historia de si fue el policía que te cacheó a las tres de la mañana el que te puso la droga en el bolsillo.

— ¿Esto es ilegal, alegal...?

— El pasado martes entró en vigor un decreto según el cual las fuerzas del orden público pueden usar virus y troyanos para acceder a usuarios. Desde 2011 a 2015 ya tenían la tecnología para hacerlo aunque no era legal. Ahora desde hace dos días ya es legal.

— ¿Usted cómo se protege?

— Yo como empresario cuando estoy realizando operaciones sensibles dejo el *smartphone* en casa y uso un Nokia de hace quince años, sin internet y con una tarjeta prepago que me dio un agente del CNI, que la compró en Lavapiés a nombre de una señora rumana. Así no pueden entrar en mi teléfono ni geolocalizarme de forma exacta. En el libro cuento que los servicios secretos han prohibido a Obama tener iPhone. Y es que según la Patriot Act, sin autorización judicial las compañías americanas (Apple, Google, Facebook...) están obligadas a dar toda la información (correos, llamadas...) que conozcan sobre un individuo, estadounidense o no. A Obama le prohíben usar iPhone y nosotros le damos uno a cada diputado.

"Vivimos felices al no ser conscientes de todo lo que la tecnología puede hacer en nuestra contra"

"Con un ordenador un tío en Pakistán puede hacer saltar por los aires una central nuclear"

"En España falta talento informático. Tras lo de París, el CNI ha contratado hackers de Europa del Este"